

EXAMINING FEDERAL SCIENCE AGENCY
ACTIONS TO SECURE THE U.S.
SCIENCE AND TECHNOLOGY ENTERPRISE

HEARING
BEFORE THE
COMMITTEE ON SCIENCE, SPACE,
AND TECHNOLOGY
OF THE
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
SECOND SESSION

FEBRUARY 15, 2024

Serial No. 118-34

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

54-779PDF

WASHINGTON : 2026

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. FRANK LUCAS, Oklahoma, *Chairman*

BILL POSEY, Florida	ZOE LOFGREN, California, <i>Ranking Member</i>
RANDY WEBER, Texas	SUZANNE BONAMICI, Oregon
BRIAN BABIN, Texas	HALEY STEVENS, Michigan
JIM BAIRD, Indiana	JAMAAL BOWMAN, New York
DANIEL WEBSTER, Florida	DEBORAH ROSS, North Carolina
MIKE GARCIA, California	ERIC SORENSEN, Illinois
STEPHANIE BICE, Oklahoma	ANDREA SALINAS, Oregon
JAY OBERNOLTE, California	VALERIE FOUSHEE, North Carolina
CHUCK FLEISCHMANN, Tennessee	KEVIN MULLIN, California
DARRELL ISSA, California	JEFF JACKSON, North Carolina
RICK CRAWFORD, Arkansas	EMILIA SYKES, Ohio
CLAUDIA TENNEY, New York	MAXWELL FROST, Florida
RYAN ZINKE, Montana	YADIRA CARAVEO, Colorado
SCOTT FRANKLIN, Florida	SUMMER LEE, Pennsylvania
DALE STRONG, Alabama	JENNIFER McCLELLAN, Virginia
MAX MILLER, Ohio	GABE AMO, Rhode Island
RICH MCCORMICK, Georgia	SEAN CASTEN, Illinois,
MIKE COLLINS, Georgia	<i>Vice Ranking Member</i>
BRANDON WILLIAMS, New York	PAUL TONKO, New York
TOM KEAN, New Jersey	
VACANCY	

C O N T E N T S

February 15, 2024

	Page
Hearing Charter	2
Opening Statements	
Statement by Representative Frank Lucas, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	13
Written Statement	14
Statement by Representative Zoe Lofgren, Ranking Member, Committee on Science, Space, and Technology, U.S. House of Representatives	15
Written Statement	17
Witnesses:	
The Honorable Arati Prabhakar, Director, White House Office of Science and Technology Policy	18
Oral Statement	21
Written Statement	21
Dr. Rebecca Keiser, Chief of Research Security Strategy and Policy, National Science Foundation	26
Oral Statement	26
Written Statement	28
Dr. Geri Richmond, Under Secretary for Science and Innovation, Department of Energy	35
Oral Statement	35
Written Statement	37
Dr. Michael Lauer, Deputy Director for Extramural Research, National Insti- tutes of Health	45
Oral Statement	45
Written Statement	47
Discussion	51
Appendix I: Answers to Post-Hearing Questions	
The Honorable Arati Prabhakar, Director, White House Office of Science and Technology Policy	88
Dr. Rebecca Keiser, Chief of Research Security Strategy and Policy, National Science Foundation	102
Dr. Geri Richmond, Under Secretary for Science and Innovation, Department of Energy	111
Dr. Michael Lauer, Deputy Director for Extramural Research, National Insti- tutes of Health	125
Appendix II: Additional Material for the Record	
Documents submitted by Representative Frank Lucas, Chairman, Committee on Science, Space, and Technology, U.S. House of Representatives	142
Statement from the Association of American Universities	142
Letter from Barbara R. Snyder, President, the Association of American Universities, to Dr. Arati Prabhakar, Director, White House Office of Science and Technology Policy	146

IV

	Page
Report submitted by Representative Bill Posey, Committee on Science, Space, and Technology, U.S. House of Representatives	
“Research Security: Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats,” United States Government Accountability Office	148

**EXAMINING FEDERAL SCIENCE AGENCY
ACTIONS TO SECURE THE U.S. SCIENCE
AND TECHNOLOGY ENTERPRISE**

THURSDAY, FEBRUARY 15, 2024

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Committee met, pursuant to notice, at 10:01 a.m., in room 2318 of the Rayburn House Office Building, Hon. Frank Lucas [Chairman of the Committee] presiding.

**FULL COMMITTEE****HEARING CHARTER**

“Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise”

Thursday, February 15, 2024

10:00 a.m. – 12:00 p.m.

2318 Rayburn House Office Building

Purpose

The purpose of this hearing is to examine the actions taken by federal science agencies to implement recent guidance and laws to protect proprietary technology and scientific discoveries, including the *Guidance for Implementing NSPM-33 on National Security Strategy for United States Government-Supported Research and Development* and the research security provisions in the 2020 and 2021 National Defense Authorization Acts and the Chips and Science Act of 2022. The Committee will discuss the status of implementation of these provisions across the federal government, barriers to compliance, as well as newly identified risks and threats to the security of federally funded research. The hearing will also examine the implications of undue foreign influence for researchers, research institutions, and the competitiveness of the U.S. research enterprise.

Witnesses

- **The Honorable Arati Prabhakar**, Director, White House Office of Science and Technology Policy
- **Dr. Rebecca Keiser**, Chief of Research Security Strategy and Policy, National Science Foundation
- **The Honorable Geri Richmond**, Under Secretary for Science and Innovation, Department of Energy
- **Dr. Michael Lauer**, Deputy Director for Extramural Research, National Institute of Health

Overarching Questions

- What is the status of research security activities at federal science agencies? What is the timeline for full compliance with existing statutes and executive branch guidance?
- How are federal science agencies coordinating to ensure uniformity in the implementation of research security guidance and requirements?
- How are federal science agencies and the broader research community engaging with law enforcement and the intelligence community to understand and address the threat of malicious actors exploiting our open system of science?
- What actions are being taken to engage with the broad research community to communicate appropriate training requirements and best practices for identifying research security risks?
- Why is it important for the U.S. to balance security risks and the importance of scientific openness and international collaboration? How will our implementation of research security requirements impact U.S. competitiveness?

BACKGROUND

Openness is one of the most important tenets of scientific research. Broad dissemination of results and data and the free exchange of ideas facilitate wider evaluation and confirmation of results and spark new collaborations and avenues of inquiry. Openness increases the validity of research results, improves productivity and student training, and helps deliver the benefits of research to the broader public. It also enables the scientific community to identify and correct for instances of scientific misconduct, such as fabrication or falsification of data, enhancing the integrity of the entire research enterprise and building accountability and public trust.

While there are domains in which openness in science can be detrimental to national competitiveness or security, fundamental research has been generally exempted from security restrictions since 1985. President Reagan's National Security Decision Directive 189 (NSDD-189) defines fundamental research as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons." It also dictates that "to the maximum extent possible, the products of fundamental research remain unrestricted," and specifies that "where the national security requires control, the mechanism for control of information generated during federally funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification."¹

The directive does not claim that the open sharing of fundamental research is without risk. Rather, it asserts that openness in research is so important to competitiveness and security that it warrants the risk that adversaries may benefit from scientific openness as well.

¹ The White House. (1985, September 21). NSDD 189 National Policy on Transfer of Scientific, Technical and Engineering Information. National Archives Catalog. <https://catalog.archives.gov/id/6879779>.

In recent years, several incidents have led to the concern that other countries are taking advantage of the openness of the academic research environment in the United States, underscoring the need to balance a commitment to openness with the potential threats posed by foreign actors seeking to exploit, degrade and misappropriate America's open system of science.² Threats to research security primarily arise from the failure of researchers applying for federal funding to disclose foreign affiliations, such as participation in a foreign talent recruitment program, conflicts of commitments, and sources of funding that may present a conflict of interest (COI). Because federal science agencies award research grants to institutions, not the individual researcher, institutions are primarily responsible for ensuring compliance with these policies.

Funding agencies are usually alerted to allegations of noncompliance, through notification from the awardee's institution, an anonymous tip, or another audit or investigation. At that point they coordinate with the institution to assess the available evidence and determine if an agency action is necessary. In many cases, an agency works with the university and researcher to bring them into compliance and ensure expectations are clearly communicated. If the agency suspects a researcher engaged in intentional deception, misconduct, or fraud, the agency can refer the case to the Office of the Inspector General (OIG) for further investigation. In addition, the OIG can and does initiate its own investigations, and when appropriate, refers criminal cases to the Department of Justice (DOJ).

Research integrity is a set of ethical standards that form the foundation for responsible conduct of research: objectivity, honesty, openness, accountability, fairness, and stewardship.³ Research security can be defined as "safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity and foreign government interference."⁴ For example, malign foreign talent recruitment programs have been found to incentivize or coerce participants to acquire "through illicit as well as licit means, proprietary technology or software, unpublished data and methods, and intellectual property to further the military modernization goals and/or economic goals of a foreign government."⁵ Funding agencies and DOJ have identified and cracked down on several specific behaviors, including:

- failure to disclose conflicts of financial and non-financial interest, including funding, parallel laboratories, employment, affiliations, and appointments;

² JASON, The MITRE Corporation. *Fundamental Research Security*. December 2019. McLean, VA. Available at https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

³ National Academies of Sciences, Engineering, and Medicine. 2017. *Fostering Integrity in Research*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/21896>.

⁴ National Science and Technology Council, Subcommittee on Research Security and Joint Committee on the Research Environment. "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development," January 2022, available at <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>.

⁵ National Science & Technology Council, Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise. January 2021. Available at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf>.

- failure by peer reviewers to keep information in grant applications confidential, including disclosure to foreign entities or other attempts to influence funding decisions; and
- diversion of intellectual property in grant applications or produced by agency-supported research to other entities, including other countries.

Participation in a foreign talent recruitment program is not necessarily improper. However, in recent years, research funding agencies have uncovered a correlation between noncompliance with COI and disclosure requirements and participation in Chinese-government sponsored malign talent recruitment programs.⁶

EXECUTIVE BRANCH ACTIONS

White House Office of Science and Technology Policy and Interagency Workgroups

In the last few years, multiple government entities have written or commissioned guidance documents in an attempt to define known threats to the U.S. research enterprise.

In February 2019, then-Director of the White House Office of Science and Technology Policy (OSTP), Kelvin Droegemeier, announced that “ensuring the safety and security of researchers and our innovations” was among OSTP’s top policy priorities.⁷ As OSTP Director, Droegemeier also served as chair of the National Science and Technology Council (NSTC) – a cabinet-level advisory body composed of representatives from federal science agencies that was created by executive order to coordinate science and technology (S&T) policy.⁸ Historically, OSTP and the NSTC have worked together to coordinate the development and implementation of research and development (R&D) policies across federal science agencies. In keeping with this precedent, the NSTC convened a new body of agency representatives to prioritize the coordination of research security policies.

In May 2019, the NSTC formed the Joint Committee on Research Environments (JCORE) “to address the most pressing challenges facing America’s research and scientific community.”⁹ JCORE established four subcommittees to coordinate its work: the Subcommittee on Safe and Inclusive Research Environments, the Subcommittee on Rigor and Integrity in Research, the Subcommittee on Reducing Administrative Burdens, and the Subcommittee on Research Security.¹⁰

⁶ *Id.*

⁷ Droegemeier quoted in William Thomas, “Droegemeier Outlines Agenda in First Speech as OSTP Director,” FYI: Science Policy News, February 20, 2019, <https://ww2.aip.org/fyi/2019/droegemeier-outlines-agenda-first-speech-ostp-director>.

⁸ CRS Report R47635, *The White House Office of Science and Technology Policy: Issues and Options for the 118th Congress*, by Emily G. Blevins and Rachael F. Roan.

⁹ The White House Office of Science and Technology Policy, Update from the National Science and Technology Council Joint Committee on Research Environments, July 9, 2019, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2019/07/Update-from-the-NSTC-Joint-Committee-on-Research-Environments-July-2019.pdf>.

¹⁰ *Id.*

In December 2019, just over six months after its launch, Congress codified the ongoing work of the NSTC's JCORE Subcommittee on Research Security in the "Securing American Science and Technology Act" as part of the National Defense Authorization Act (NDAA) for Fiscal Year 2020.¹¹ The bill also directed the National Science Foundation (NSF), the Department of Energy (DOE), the Department of Defense (DOD), and other agencies to enter into a joint agreement with the National Academies of Science, Engineering, and Medicine to establish a National Science, Technology, and Security Roundtable to identify best practices for communicating threats and risks to federally funded R&D, among other purposes.¹²

On January 14, 2021, President Trump issued National Security Presidential Memorandum 33 (NSPM-33), "*Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*," which tasked OSTP and the Subcommittee on Research Security with coordinating the implementation of these provisions across federal agencies to secure federally funded R&D.¹³ NSPM-33 directs actions by funding agencies to secure intellectual capital while acknowledging the importance of openness and scientific collaboration. These include:

- prohibiting Federal personnel from participating in foreign-government-sponsored talent recruitment programs;
- requiring institutions of higher education to develop research security programs;
- directing agencies and universities to share information about individuals whose behavior poses a risk to research integrity and security;
- directing the Department of State and the Department of Homeland Security to review vetting processes for foreign students and researchers;
- directing agencies to harmonize disclosure processes and definitions; and
- streamlining the grant application process through the use of digital persistent identifiers (DPI).

In response, OSTP and the Subcommittee on Research Security have issued several publications containing guidance for federal agencies to implement the research security requirements outlined in NSPM-33, including the following:

- NSTC JCORE Subcommittee on Research Security, *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*, January 2021;¹⁴
- White House, OSTP, NSPM-33 Fact Sheet, "President Trump Takes Bold Action to Strengthen the Security and Integrity of America's Research and Development Enterprise," January 2021;¹⁵

¹¹ [P.L. 116-92](#), Div. A, Title XVII, §1746(a).

¹² [P.L. 116-92](#), Div. A, Title XVII, §1746(b).

¹³ The White House, "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," January 14, 2021, <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>.

¹⁴ *supra* note 5

¹⁵ The White House, *President Trump Takes Bold Action to Strengthen the Security and Integrity of America's*

- White House, OSTP Blog Post by Eric Lander, “Clear Rules for Research Security and Researcher Responsibility,” August 10, 2021;¹⁶
- White House, OSTP Blog Post by Eric Lander, “Guidance for U.S. Scientific Research Security That Preserves International Collaboration,” January 4, 2022;¹⁷
- NSTC JCORE Subcommittee on Research Security, Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States-Government-Supported Research and Development, January 2022;¹⁸
- Memorandum from Alondra R. Nelson, Deputy Director for Science and Society, OSTP, to Heads of Member Agencies of the National Science and Technology Council, “Re: Next Steps on NSPM-33 Implementation,” March 1, 2022;¹⁹ and
- White House, OSTP, Updates on Research Security Policies and Practices in the U.S. Government, October 2022.²⁰

In February 2023, the NSTC Subcommittee on Research Security released a “Draft Research Security Programs Standard Requirement” to facilitate implementation of Section 4(g) of NSPM-33.²¹ The draft guidance provided additional details on covered organizations, foreign travel security, research security training, cybersecurity, and export control training. It also specified that federal agencies should communicate the required training components and standards to research organizations as part of their funding agreement processes. A revised version of the draft guidance was posted in the Federal Register for public comment on March 7, 2023.²²

National Science Foundation

In December 2019, JASON issued an NSF-commissioned report titled “Fundamental Research Security”.²³ JASON is an independent science advisory group that contracts with government

Research and Development Enterprise. January 2021. Fact Sheet. Available at <https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSC-OSTP-NSPM33-Fact-Sheet-Jan2021.pdf>.

¹⁶ Lander, E. (2021, August 10). Clear rules for research security and researcher responsibility. The White House. <https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/>

¹⁷ Lander, E. (2022, January 4). Guidance for U.S. Scientific Research Security that preserves international collaboration. The White House. <https://www.whitehouse.gov/ostp/news-updates/2022/01/04/guidance-for-u-s-scientific-research-security-that-preserves-international-collaboration/>

¹⁸ *supra* note 4.

¹⁹ Office of Science and Technology Policy, & Nelson, A., White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/03/03-2022-Coordination_RS_Letter.pdf.

²⁰ Executive Office of the President of the United States, Updates on Research Security Policies and Practices in the U.S. Government. Office of Science and Technology Policy. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/10/WHOSTP_ResearchSecurity_CommunityBriefingSlides.pdf.

²¹ NSTC Subcommittee on Research Security, “Draft Research Security Programs Standard Requirement,” February 2023, https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

²² OSTP, Request for Information: NSPM 33 Research Security Programs Standard Requirement, 88 Federal Register 14187, April 7, 2023, <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement>.

²³ Long, G., National Science Foundation (2019). The MITRE Corporation. Retrieved February 7, 2024, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-21FundamentalResearchSecurity_12062019FINAL.pdf.

agencies to produce reports on matters of defense science and technology.²⁴ The report affirmed the importance of foreign scientific talent, warned against placing new restrictions on access to fundamental research, and acknowledged the difficulty in assessing the scale and scope of legitimate threats to research security. It concluded by stating that “many of the problems of foreign influence that have been identified are ones that can be addressed within the framework of research integrity.”

Prior to the JASON report, NSF issued a policy prohibiting NSF employees and rotators from participating in foreign talent recruitment programs in July 2019.²⁵ Then in February 2020, NSF clarified that its disclosure requirement for grant applicants includes both foreign and domestic sources of support.²⁶ In March 2020, NSF established a new Chief of Research Security Strategy and Policy position.²⁷

In September 2021, in partnership with the National Institute of Health (NIH), NSF implemented a new digital format for submitting researcher biographical sketches as part of grant applications to simplify and standardize the disclosure process for researchers seeking funding from both agencies.²⁸ Then, acting on behalf of the Subcommittee on Research Security, in August 2022, NSF released two draft common disclosure forms for public comment to enhance disclosure requirements and reduce the administrative burden on grant applicants.²⁹ NSF released the final versions³⁰ of the common disclosure forms along with an updated list of relevant definitions in November 2023.³¹

NSF has also updated its draft version of the Proposal and Award Policies and Procedures Guide to include requirements for institutions of higher education to disclose current financial support of \$50,000 or more from a foreign source, directly or indirectly.³² Most recently, NSF launched

²⁴ Aftergood, St. (Ed.). (n.d.). Jason Defense Advisory Panel reports. JASON Defense Advisory Panel: Reports on Defense Science and Technology. <https://irp.fas.org/agency/dod/jason/>.

²⁵ Office of the Director, Personnel Policy on Foreign Government Talent Recruitment Programs (2019). National Science Foundation. Retrieved from https://www.nsf.gov/bfa/dias/policy/researchprotection/PersonnelPolicyForeignGovTalentRecruitment%20Programs07_11_2019.pdf.

²⁶ NSF Grants. (2020b, February 18). 2/6/20 PAPPG webinar - training for the External Community. YouTube. <https://www.youtube.com/watch?v=OeZHhoHTqf4>.

²⁷ NSF News - NSF creates new research security chief position. NSF. (2020, March 2). <https://new.nsf.gov/news/nsf-creates-new-research-security-chief-position>

²⁸ Documents required for senior personnel. NSF. (n.d.). <https://new.nsf.gov/funding/senior-personnel-documents#biographical-sketch-0bd>.

²⁹ National Science Foundation on behalf of the National Science and Technology Council's Research Security Subcommittee, “Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support,” 87 *Federal Register* 53505-53507, August 31, 2022.

³⁰ NSF, “NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization,” https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp.

³¹ NSF, National Security Presidential Memorandum-33 Implementation Guidance Appendix: Definitions, November 1, 2023, <https://www.nsf.gov/bfa/dias/policy/researchprotection/nspm33definitions.pdf>.

³² National Science Foundation, “Agency Information Collection Activities: Comment Request; National Science Foundation Proposal/Award Information-NSF Proposal and Award Policies and Procedures Guide,” 88 *Federal Register* 22488, April 13, 2023, <https://www.federalregister.gov/documents/2023/04/13/2023-07780/agency-information-collection-activities-comment-request-national-science-foundation-proposalaward>.

four interactive online research security training modules for U.S. researchers and institutions to provide clear guidelines and effective strategies to protect against existing and emerging threats.³³

National Institutes of Health

NIH established a Working Group on Foreign Influence on Research Integrity, which released a report in December 2018 with recommendations for NIH and universities on raising awareness of foreign influence and safeguarding research integrity.³⁴ NIH then issued a reminder to the research community of their full disclosure requirements in March 2018.³⁵ In 2020, NIH issued policies and provided internal training to protect confidentiality in the peer review process.^{36, 37} In December 2022, NIH partnered with NSF to fund the four research security training module awards focused on the importance of research security, the importance of disclosure, risk management and mitigation, and international collaboration (also referred to in the NSF section.)³⁸

Congress has directed individual agencies to develop risk assessment tools and frameworks to manage and mitigate security risks. Currently, nearly each agency has developed and operates their own risk assessment tools. One such example is, as part of the Consolidated Appropriations Act of 2023,³⁹ Congress directed the Department of Health and Human Services (HHS) to develop a comprehensive framework and policies for assessing and managing national security risks before and after making funding awards as well as risks associated with granting access to data that may pose national security concerns.

Department of Energy

In a December 2018 memo, DOE affirmed the importance of research collaboration but raised alarms about foreign influence. The memo established a DOE S&T Risk Matrix, which identifies emerging research areas and technologies subject to restricted access by and collaboration with “sensitive country foreign nationals.” The Risk Matrix is being used by the agency but is not publicly accessible. The Risk Matrix was formally codified into law with the passage of the CHIPS and Science Act. DOE also set up a Federal Oversight Advisory Body (FOAB) to

³³ NSF Research Security Training Modules Now available. NSF. (2024, January 30). <https://new.nsf.gov/news/nsf-research-security-training-modules>.

³⁴ NIH Advisory Committee to the Director, ACD Working Group for Foreign Influences on Research Integrity (2018). National Institute of Health. Retrieved from https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf.

³⁵ U.S. Department of Health and Human Services. (n.d.). Financial conflict of interest: Investigator disclosures of foreign financial interests. National Institutes of Health. <https://grants.nih.gov/grants/guide/notice-files/NOT-OD-18-160.html>.

³⁶ NIH, “Grants and Funding: Review Guidelines,” November 19, 2020, available at <https://grants.nih.gov/grants/policy/review-guidelines.htm>.

³⁷ NIH Grants. (2020, November 9). Master class in review integrity. YouTube. <https://www.youtube.com/watch?v=X0yvzUUC9yY>.

³⁸ NSF 2022 research security training for the United States Research Community Awardees announced. NSF. (2022, December 9). <https://new.nsf.gov/news/nsf-2022-research-security-training-united-states>.

³⁹ P.L. 117-328

maintain the Risk Matrix and process exemption requests.⁴⁰ In June 2019, DOE issued a directive prohibiting DOE employees and contractors from participating in foreign talent recruitment programs sponsored by China, Iran, North Korea, and Russia.⁴¹

Additionally, DOE provided several other directives to continue protecting its resources. DOE has policies regarding foreign nationals' accessibility to the National Laboratories to ensure that even in an unclassified environment the federal government is protecting its investments.⁴² DOE also added a requirement that anyone receiving funding from an agency must report if they have any conflict of interests that may undermine the DOE research enterprise.⁴³ Lastly, unlike most research agencies, DOE is a participating member of the intelligence community. This allows DOE to use unique tools to ensure its organization is secure.

RESEARCH UNIVERSITIES

The capacity to respond to research security risks varies depending on the resources, staffing, and expertise available at each institution. Some universities have set up new research security programs dedicated to identifying and mitigating risks in coordination with the IC, law enforcement, and research funding agencies. Smaller institutions are focused on raising awareness and keeping up with the patchwork of new requirements. A fall 2019 survey describes the range of activities on university campuses.⁴⁴ However, many universities are awaiting guidance from the federal government on the requirements for institutional programs to certify compliance with NSPM-33 directives, including the draft guidance OSTP noticed in the federal register in March 2023.⁴⁵ In the last 11 months, many institutions have been left in limbo and have requested OSTP hold listening sessions to receive feedback on the proposed research security programs standard guidance.⁴⁶

⁴⁰ U.S. Department of Energy, UNCLASSIFIED FOREIGN NATIONAL ACCESS PROGRAM (2021). Retrieved from <https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b-chg1-ltdchg/@images/file>.

⁴¹ LaBarge, J. (2021, April 23). Doe O 486.1. Department of Energy Foreign Government Talent Recruitment Programs. Department of Energy Foreign Government Talent Recruitment Programs - DOE Directives, Guidance, and Delegations. <https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder>.

⁴² Emanuelson, J. (2022, March 3). Doe O 142.3b CHG 1 (LtdChg), Unclassified Foreign National Access Program. Unclassified Foreign National Access Program - DOE Directives, Guidance, and Delegations. <https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b-chg1-ltdchg>.

⁴³ Ison, J. (2021, July 9). Doe O 486.1A, foreign government sponsored or affiliated activities. Foreign Government Sponsored or Affiliated Activities - DOE Directives, Guidance, and Delegations. <https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder-a>.

⁴⁴ University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus. (2020, May). Association of American Universities. Retrieved from <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf>.

⁴⁵ OSTP, Request for Information; NSPM 33 Research Security Programs Standard Requirement, 88 Federal Register 14187, April 7, 2023, <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement>.

⁴⁶ Smith, T., & Asbury, M. (2023, May 31). Request for Information; NSPM 33 Research Security Programs Standard Requirement. Association of American Universities. Retrieved from

RECENT CONGRESSIONAL ACTIONS

Over the past four years, the Science, Space, and Technology Committee has worked to address many of these research security concerns and build a more effective and resilient R&D ecosystem. This Committee has consistently strived to balance security risks and the importance of scientific openness and international collaboration. Some of the legislative actions take include:

Securing American Science and Technology Act ⁴⁷ established an interagency committee within the White House Office of Science and Technology Policy (OSTP) to coordinate research security across the Federal government. It also established the National Science, Technology, and Security Roundtable at the National Academy of Sciences to facilitate collaboration between universities, federal agencies, law enforcement, and other stakeholders.

Disclosure Requirements for Federal Science Agencies

The Government Accountability Office (GAO) issued a report in December 2020 assessing the COI and disclosure policies at NSF, NIH, the National Aeronautics and Space Administration (NASA), DOD, DOE, and 11 universities.⁴⁸ GAO found that all five agencies require researchers to disclose information as part of their grant proposal but that there was variability in the policies and agencies lack clear enforcement mechanisms. GAO also concluded that, due to differing policies and inconsistent implementation, researchers may be unsure of what they need to disclose. In response, DOE established an interim COI policy on December 20, 2021,⁴⁹ and NASA updated their COI policy on August 31, 2023.⁵⁰

In response to this report, in January 2021, as part of the NDAA for Fiscal Year 2021, Congress moved to standardize disclosure policies by mandating that each federal agency require individuals applying for federal R&D funding to disclose all current and pending research support during the application process.⁵¹ Congress also charged OSTP, acting through the NSTC Research Security Subcommittee, with ensuring the consistency of such requirements established by federal agencies.⁵²

<https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Science%20%26%20Security/NSPM-33%20RSPS%20AAU%20Comments.pdf>.

⁴⁷ P.L. 116-92, Div. A, Title XVII, §1746(a).

⁴⁸ U.S. Government Accountability Office, "Federal Research Agencies need to Enhance Policies to Address Foreign Influence," December 17, 2020, available at <https://www.gao.gov/assets/gao-21-130.pdf>.

⁴⁹ DOE, "DOE Interim Conflict of Interest Policy," <https://www.energy.gov/sites/default/files/2022-10/Department%20of%20Energy%20Interim%20Conflict%20of%20Interest%20Policy.pdf>.

⁵⁰ NASA, "Conflict of Interest Policy for Recipients of NASA Financial Assistance Awards," 88 Federal Register 60243, August 31, 2023, <https://www.federalregister.gov/documents/2023/08/31/2023-18802/conflict-of-interest-policy-for-recipients-of-nasa-financial-assistance-awards>.

⁵¹ Section 223, National Defense Authorization Act for Fiscal Year 2021 (P.L. 116-283); 42 U.S.C. §6605.

⁵² P.L. 116-283, Div. A, Title II,

*CHIPS and Science Act of 2022*⁵³

- Prohibits all federally funded research grantees from being a member of a malign foreign talent program or participating in similar activities.
- Prohibits federal agency personnel from participating in foreign talent programs and requires researchers working on federally funded research projects to disclose any participation in foreign talent recruitment programs.
- Requires all federally funded grantees to take annual training on research policies and foreign threats and directs OSTP to work with NSF and NIH to develop training for all grantees across the Federal research agencies.
- Directs NSF to develop a plan to identify research areas that may involve access to classified or controlled unclassified information and to exercise due diligence processes in granting access to such information.
- Bans NSF funding from going to organizations hosting Confucius Institutes.
- Creates an Office of Research Security and Policy at NSF and gives the office and the Inspector General additional resources and new authorities to use analytical tools to detect and combat foreign influence, theft, and grant fraud.
- Gives Federal research agencies the authority to require the submission of supporting documentation and the authority to act on findings that identify undue foreign influence or grant fraud.
- Directs NSF to collect annual summaries of foreign financial support from universities and grants NSF the authority to request copies of contracts or documentation related to such disclosures.
- Directs NIST to assist universities in adopting the Cybersecurity Framework to help mitigate cybersecurity risks related to conducting research. In addition, title III directs the development of a national secure computing enclaves program to protect sensitive research information at American universities from cyber theft.

⁵³ [P.L. 117-167](#), Title III, Subtitle D; and Title VI, Subtitle D.

Chairman LUCAS. The Committee will come to order. Without objection, the Chair is authorized to declare recesses of the Committee at any time.

Welcome to today's hearing entitled "Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise." I recognize myself for 5 minutes for an opening statement.

Thank you for joining us at this hearing on research security and protecting our taxpayer investments. Research theft is one of the single greatest threats to our competitiveness as a nation. It takes our hard-won innovation and puts it to work for our adversaries, hurting our economy and our ability to stay at the leading edge of tech discovery.

This is no idle threat either. China has been explicit about their efforts to steal the results of our research to further their own technological progress. The Chinese Communist Party has made it clear they intend to surpass us as the global leader in science and technology (S&T), and they have no qualms about using intellectual property theft, forced technology acquisition, and other illicit means to do so.

That's why this Committee has been proactive in our response to this threat and has passed multiple bills to protect American research. In the 2020 *NDAA (National Defense Authorization Act)*, we passed the *Securing American Science and Technology Act*, which established an interagency committee within the White House Office of Science and Technology Policy (OSTP) to coordinate research security across the Federal Government. That same year, the Trump Administration released National Security Presidential Memorandum (NSPM) 33 to direct a national response to protect our research and technology.

In 2021, we went even further and began requiring all Federal R&D (research and development) funding applicants to disclose all of their sources of support, ensuring there are consistent conflict-of-interest policies across agencies. And in 2022, we passed several research security protections as a part of *CHIPS and Science Act* to halt the theft of U.S. innovation. We banned participation in malign foreign talent programs designed to recruit researchers to work for our adversaries. We also required plans to protect sensitive basic research and created an Office of Research Security and Policy at the NSF (National Science Foundation).

Taken together, these measures provide a strong framework for research security, but to be of any use in protecting our investments, the Administration needs to actually execute this framework. Four years ago, we directed OSTP to coordinate and harmonize research security across the Federal Government. In that time, some progress was made, and while I'm pleased that this hearing sparked the release of three different policy guidance memos yesterday, congressional deadlines were missed, and there's work still to be done.

The government needs to have timely, clear, and uniform guidance on this issue for our agencies and our researchers. It's unacceptable that we don't have that. We've heard from agencies and stakeholders saying they are having trouble implementing their own research security guidelines because there are no government-wide standards yet. I'd like to request unanimous consent to enter

into the record this statement from the Association of American Universities (AAU), as well as a letter sent by the AAU's President Barbara Snyder to Dr. Prabhakar earlier this week.

Seeing no objection, so ordered.

This letter states that since the June 2023 comment deadline, OSTP has not released final requirements or an update to the research community on the status of finalizing the requirements of research security programs. It goes on to emphasize the importance of harmonizing these requirements across the Federal Government and encourages OSTP to finalize the requirements as soon as possible. So, today, I expect to hear more about this work, and I'm hoping to get answers on why we aren't further along in this process.

I understand that this is a complicated endeavor. America's strength in science and technology has been driven by our unique research ecosystem, which combines Federal, academic, and private R&D efforts. For that system to work, we need a degree of open science that facilitates collaboration and transparency.

I also want to be clear, we're not here to target researchers based on their race, but based on the actions they have taken. Our goal is to ensure that all federally funded scientists follow the U.S. principles of scientific fairness and integrity. The United States has benefited greatly from international scientific collaboration and the contribution of foreign-born scientists. I want the United States to remain a desirable place for brilliant minds to come and share their ideas. That's what makes us different than China. We celebrate freedom of thought, and when possible, we share information in good faith so we can maximize innovation. Our challenge is preserving this culture of transparency and openness, particularly when it comes to basic research, while protecting the sensitive information that could benefit our adversaries. I believe that we are up to this challenge.

I look forward to hearing from our witnesses today on how we can continue to keep America's R&D strong and productive.

[The prepared statement of Chairman Lucas follows:]

Thank you for joining us at this hearing on research security and protecting our taxpayer investments.

Research theft is one of the single greatest threats to our competitiveness as a nation. It takes our hard-won innovation and puts it to work for our adversaries, hurting our economy and our ability to stay at the leading edge of discovery.

This is no idle threat either. China has been explicit about their efforts to steal the results of our research to further their own technological progress.

The Chinese Communist Party has made it clear that they intend to surpass us as the global leader in science and technology, and they have no qualms about using intellectual property theft, forced technology acquisition, and other illicit means to do so. That's why this Committee has been proactive in our response to this threat and has passed multiple bills to protect American research.

In the 2020 NDAA we passed the *Securing American Science and Technology Act*, which established an interagency committee within the White House Office of Science and Technology Policy to coordinate research security across the federal government.

That same year, the Trump Administration released National Security Presidential Memorandum-33 to direct a national response to protect our research and technology.

In 2021 we went even further and began requiring all federal R&D funding applicants to disclose all of their sources of support, ensuring there are consistent conflict of interest policies across agencies.

And in 2022 we passed several research security protections as part of the *CHIPS and Science Act* to halt the theft of U.S. innovation.

We banned participation in malign foreign talent programs designed to recruit researchers to work for our adversaries.

We also required plans to protect sensitive basic research and created an Office of Research Security and Policy at NSF.

Taken together, these measures provide a strong framework for research security. But to be of any use in protecting our investments, the Administration needs to actually execute this framework.

Four years ago we directed OSTP to coordinate and harmonize research security across the federal government. In that time, some progress was made. And while I am pleased that this hearing sparked the release of three different policy guidance memos yesterday, congressional deadlines were missed and there is work still to be done.

The government needs to have timely, clear, and uniform guidance on this issue for our agencies and for our researchers.

It's unacceptable that we don't have that. We've heard from agencies and stakeholders saying they are having trouble implementing their own research security guidelines because there are no government-wide standards yet.

I would like to request Unanimous Consent to enter into the record this statement from the Association of American Universities, as well as a letter sent by AAU's President, Barbara Snyder, to Dr. Prabhakar earlier this week.

This letter states that, "since the June 2023 comment deadline, OSTP has not released final requirements or an update to the research community on the status of finalizing" the requirements for research security programs.

It goes on to emphasize the importance of harmonizing these requirements across the federal government and encourages OSTP to finalize the requirements as soon as possible.

So today I expect to hear more about this work and I'm hoping to get answers on why we aren't further along in this process.

I understand that this is a complicated endeavor. America's strength in science and technology has been driven by our unique research ecosystem, which combines federal, academic, and private R&D efforts.

For that system to work, we need a degree of open science that facilitates collaboration and transparency.

I also want to be clear; we are not here to target researchers based on their race but based on the actions they have taken. Our goal is to ensure that all federally funded scientists follow the U.S. principles of scientific fairness and integrity.

The U.S. has benefitted greatly from international scientific collaboration and the contributions of foreign-born scientists.

I want the U.S. to remain a desirable place for brilliant minds to come and share their ideas.

That's what makes us different than China. We celebrate freedom of thought. And when possible, we share information in good faith so that we can maximize innovation.

Our challenge is preserving this culture of transparency and openness—particularly when it comes to basic research—while protecting the sensitive information that could benefit our adversaries.

I believe that we are up to this challenge. I look forward to hearing from our witnesses today on how we can continue to keep America's R&D strong and productive.

Chairman LUCAS. And with that, I yield back and recognize the Ranking Member, the gentlewoman from California, for an opening statement.

Ms. LOFGREN. Well, thank you, Chairman Lucas, and for today's hearing, and I'd like to welcome our distinguished panel of witnesses.

For several years now, really, for the history of this Committee, we've taken the lead in Congress on grappling with hard questions around emerging technologies and implications for U.S. competitiveness, national security in our society. Specifically, the question of when and how to secure federally funded research, it isn't new. We've been supporting research behind closed doors for decades because it's deemed classified or proprietary or otherwise subject to access restrictions. Everything else, certainly everything else la-

beled as fundamental research is carried out and published in the open, as affirmed by President Ronald Reagan in National Security Decision Directive 189. And that's been reaffirmed several times since.

Now, two things have changed. One is the United States is no longer the unquestioned leader in science, technology, and innovation. When we were, our risk calculus might have been different than it is now. In addition to our worthy but mostly likeminded competitors around the globe, we face a growing strategic competitor and I would say a threat from China.

The second thing is the confluence of several emerging technologies with dual-use potential, including AI (artificial intelligence), biotech, and quantum. As the landscape continues to evolve, what's most important is we continue to approach this challenge thoughtfully and clear-eyed about the tradeoffs we're willing to make and not willing to make.

Now, I'm proud of the history of this Committee doing just that. Chairman Lucas was a great partner to then-Chairwoman Johnson in developing thoughtful, widely vetted policy proposals in response to well-defined problems. For example, this Committee developed the requirement for OSTP to lead in updating and coordinating the disparate and confusing disclosure requirements across Federal agencies. And we also developed the requirement for Federal research security training for all federally funded researchers.

Our primary purpose for this hearing, as the Chairman has said, is to check on the implementation, and we do have some questions about whether this has been speedy enough. It also presents a hearing—this hearing—an opportunity for the Committee to continue to lead in the more esoteric, but equally important, debates about the risk calculus.

I have long experience in immigration law, and I'd like to just cite a couple of quick facts. Since 2000, 40 percent of all U.S. Nobel laureates have been foreign-born. In addition, according to an analysis from the National Foundation for American Policy, more than half of the startups valued at \$1 billion dollars or more were started by immigrants to the United States. So we don't have to close our doors in the name of securing research, but we have to preserve our global vision and be the best country in the world to be a researcher.

When it comes to scientific collaborations across borders, we all know that we can't do the biggest things all by ourselves. To solve global challenges, we need to pool global minds and resources. The COVID pandemic certainly reminded us of that.

And finally, as the Chairman has said, this isn't about targeting people by their ethnicity. Recently, I was at an event unveiling the statue of Norm Mineta, our former colleague. Norm was taken off the streets of San Jose with his family wearing his Boy Scout uniform and interned because the United States made a mistake. We confused ethnicity with loyalty. And, of course, Norm went on to be a Member of Congress, a Cabinet Secretary twice, out of the camps, walked the most decorated unit in World War II. We cannot confuse loyalty with ethnicity or race, and this Committee has a strong record of that. We need to make sure that every effort is taken to avoid profiling based on race, ethnicity, or nationality, and I think

that starts with this Committee and is in keeping with the work we have done so far because we do need to secure our national research facilities.

So I look forward to this hearing, Mr. Chairman. I thank you for holding it, and I'm sure that it will be productive. And with that, I yield back.

[The prepared statement of Ms. Lofgren follows:]

Thank you, Chairman Lucas, for holding today's hearing. I would also like to welcome our distinguished panel of witnesses.

For several years now—and really for the history of this Committee—we've taken the lead in Congress on grappling with hard questions around emerging technologies and implications for U.S. competitiveness, national security, and society.

Specifically, the question of when and how to secure Federally funded research is not new. We've been supporting research behind closed doors for decades—because it is deemed classified, proprietary, or otherwise subject to access restrictions. Everything else—certainly everything else labeled as “fundamental research”—is carried out and published in the open, as affirmed by President Ronald Reagan in National Security Decision Directive-189, and reaffirmed several times since.

Two things have changed. One is that the United States is no longer the unquestioned leader in science, technology, and innovation. When we were, our risk calculus was different than it is now. In addition to our worthy but mostly like-minded competitors around the globe, we face a growing strategic competitor—and threat—in China. The second thing is the confluence of several emerging technologies with dual-use potential, including AI, biotech, and quantum.

As the landscape continues to evolve, what's most important is that we continue to approach this challenge thoughtfully and clear-eyed about the tradeoffs we are willing and not willing to make.

I'm proud of our history on the Science Committee of doing just that. Chairman Lucas was a great partner to then-Chairwoman Johnson in developing thoughtful, widely vetted policy proposals in response to well defined problems. For example, this Committee developed the requirement for OSTP to lead in updating and coordinating the disparate and confusing disclosure requirements across Federal agencies. We also developed the requirement for research security training for all Federally funded researchers.

A primary purpose of this hearing is oversight, and we are prepared with some questions for you about why implementation of some of the requirements we put in law has been so slow. I'd also like to know how we can help. But in addition to oversight, this hearing presents an opportunity for this Committee to continue to lead in the more esoteric but equally important debate about the risk calculus of what happens if we push too far in the wrong direction.

I have long been a champion for high-skilled immigration to the U.S. Let me just cite a couple of quick facts for you. Since 2000, 40% of all U.S. Nobel laureates have been foreign-born. In addition, according to an analysis from the National Foundation for American Policy, more than half of startups valued at \$1B or more were started by immigrants. We do not have to close these doors in the name of securing our research. We can instead choose to preserve the global vision of the United States being the best country in the world to be a researcher.

Furthermore, when it comes to scientific collaborations across borders, we all know that we cannot do the biggest things alone. To solve global challenges, we need to pool global minds and resources. The Covid pandemic surely reminded us of that.

And finally, we have witnessed that the rhetoric around research security itself has been enough to send a chill across our colleges, universities, and start-ups. In particular, it has left many Asian Americans and Asian nationals feeling unwelcome and even frightened. Shamefully, our nation has gone down that dark road before. We must address real risks to our security and competitiveness.

However, in doing so we must make every effort possible to avoid profiling based on race, ethnicity, or nationality. And that starts with our rhetoric.

I thank the distinguished panel for being here with us this morning and I look forward to the discussion.

Chairman LUCAS. The gentlelady yields back. And I always appreciate her wise and insightful observations.

Let me introduce our witnesses. Our first witness today is the Honorable Arati Prabhakar, Director of the White House Office of

Science and Technology Policy, and Assistant to the President for Science and Technology. The doctor has led two different Federal R&D agencies and worked with startups, large companies, universities, government labs, and nonprofits across a wide variety of sectors to create new solutions for critical challenges.

Our next witness is Rebecca Keiser, Dr. Rebecca Keiser, Chief of Research Security Strategy and Policy for the National Science Foundation. Dr. Keiser is the first to hold this post since its creation in 2020. She is a board member of Women in Aerospace and a member of the American Academy for the Advancement of Science and has her bachelor's degree in Japanese studies, master's degree in politics of world economy—that's a fascinating subject, I would acknowledge as an ag economist—and a doctorate in international studies.

Next, we have the Honorable Geri Richmond, the Under Secretary of Science and Innovation at the Department of Energy (DOE). Dr. Richmond is also a member of the U.S. Naval Academy of Sciences and the American Academy of Arts and Sciences, and has been honored by numerous awards, including most recently the National Medal of Science in 2018.

And our final witness is Dr. Michael Lauer, the Deputy Director of the Extramural Research at the National Institutes of Health (NIH). The doctor has received numerous awards, including the NIH Equal Employment Opportunity Award of the Year and the Arthur S. Flemming Award for exceptional Federal service in the recognition of his efforts to grow a culture of learning and accountability.

And with that, I now recognize Dr. Prabhakar for 5 minutes to present her testimony. Thank you for being here.

**TESTIMONY OF THE HONORABLE ARATI PRABHAKAR,
DIRECTOR, WHITE HOUSE OFFICE
OF SCIENCE AND TECHNOLOGY POLICY**

Dr. PRABHAKAR. Thank you so much, Mr. Chairman.

Chairman Lucas, Ranking Member Lofgren, all the Members of the Committee, thank you so much for this opportunity to appear before you today. I'm really pleased to be here with my—this table full of my colleagues.

I am the President's Science and Technology Advisor and Director of the White House Office of Science and Technology Policy. As you all know very well, science, technology, and innovation have been essential to American leadership in the world for many, many decades. That simply would not have been possible without the strong and consistent bipartisan support of this Committee. I first appeared before this Committee 30 years ago when I was NIST Director, and so I've gotten to see that commitment over quite a few decades now directly.

But today, we are operating in a global strategic environment that is characterized by fierce military and economic competition. That's a competition among many actors, but I want to speak specifically about the People's Republic of China (PRC) because they are the only competitor with both the intent to reshape the global order and the ability to harness both military and economic power to advance that objective. And when you look at that economic and

military competition, technology and R&D are central to this competition.

Like every other developed and developing country, the PRC pumps funding into R&D, it pursues global partnerships, it seeks to trade in high-tech goods, but the PRC is different than other global actors because of its use of illicit, as well as licit, means to acquire foreign technologies because of its engagement in unfair competition in targeted industries, and because of its mandatory military-civil fusion.

President Biden has taken unprecedented action in the face of this situation. This Administration has levied record fines for export control violations. We've established new categories for export controls. We've expanded the controls on outbound investment from the United States in sensitive areas, and we are rebuilding America's lead in semiconductor manufacturing with the bipartisan *CHIPS and Science Act*. As well, the Department of Justice has pursued trade secret theft and economic espionage cases. All of those actions are oriented toward industry, which is the major source of significant technology development. To address research security, the Administration is implementing NSPM-33, *NDAA* provisions, and provisions of the bipartisan *CHIPS and Science Act*, just as has been described.

The purpose of all of these efforts is to make sure that universities and researchers understand our altered global landscape. The world is not the same as it was a few years ago, and that's so that they can be the first line of defense against the illicit activities in the research environment.

Now, in addition to these realities of the PRC's actions, two other factors shape our work on research security. One is a fundamental American value, that our Nation values and respects each individual, and xenophobia and racism are unacceptable. The other factor is just a practical fact. We know that immigrants to the United States and global interactions have been essential to America's pre-eminent position in research and in technology, and it clearly just wouldn't be to our advantage to create an atmosphere that is hostile to attracting the world's greatest minds, many of whom see freedom and opportunity when they see the United States.

Getting research security right has been a complex task. It's one that has required more time than expected. And I want to highlight two important steps that we have accomplished. One is releasing the common disclosure forms for researchers to submit information. That's what allows agencies then to be able to identify problems. We also have released guidelines for restricting malign foreign talent recruitment programs. That's what's accomplished at this point. What we're working on right now very—in a very focused manner is guidance for research security programs in universities. It is vital that these programs protect national security and not just create another checkbox for administrators. That's the focus of our work. This is a very significant priority for me.

I'll finish simply by saying that Congress has emphasized how important research security is. This Administration agrees on its importance, and that is why we are taking the actions that are necessary to continue American leadership in science and technology. Thank you.

[The prepared statement of Dr. Prabhakar follows:]

Testimony of Arati Prabhakar

Director of the White House Office of Science and Technology Policy and
Assistant to the President for Science and Technology
before the House Science, Space, and Technology Committee
Hearing on
“Examining Federal Science Agency Actions to Secure the U.S. Science and
Technology Enterprise”
February 15, 2024

I would like to thank Chairman Lucas, Ranking Member Lofgren, and the members of this committee for the invitation to address the subject of research security.

Before my current role as the President’s science and technology (S&T) advisor and Director of the White House Office of Science and Technology Policy (OSTP), I spent half my professional life in public service, including as Director of the Defense Advanced Research Projects Agency (DARPA) and the Director of the National Institute of Standards and Technology (NIST). The other half of my career has been in the private sector, in a couple of companies and a decade in early-stage venture capital.

When President Biden asked me to step into my current role, I immediately said “yes”. I’ve been able to contribute to American innovation from so many different places, and I know that it takes the whole ecosystem—public and private—to do big things for our country. That is how we create the advances that change Americans’ lives.

OSTP is the one place that works with, looks across, and supports the entire S&T ecosystem. Our mission is to strengthen America’s science, technology, and innovation, and to make sure the enterprise is aimed at our country’s great aspirations. These include strengthening our economy, achieving robust health and opportunity for every person, meeting the climate crisis, and bolstering global peace and stability.

Today, the global strategic environment is characterized by fierce military and economic competition among many actors. I will focus on the People’s Republic of China (PRC), because it is the only competitor with both the intent to reshape the international order and the ability to harness significant military and economic power to advance that objective. This is evident in the PRC’s actions ranging from its conduct in the South China Sea, to atrocities in Xinjiang, to its state-centric approach to product standards.

Technology and research and development (R&D) are central to this competition. I would like to put the PRC’s efforts in perspective and then outline the actions of the Biden-Harris Administration.

The PRC’s spending on R&D has grown from \$14 billion in 1996 to \$670 billion in 2021 in purchasing power parity, according to the Organisation for Economic Co-operation and Development (OECD). This is an unprecedented surge, which puts the PRC into second place behind the United States’ \$800 billion in R&D expenditures in 2021. The

PRC's spending is more than 40 percent greater than the entire European Union's R&D funding.

The PRC is pouring this funding into many fields and research facilities. Both diplomatic reporting and observations among U.S. researchers indicate how the PRC is seeking to become the focal point for many areas of R&D. These efforts include offers to host R&D activities and facilities, invitations to participate in PRC experiments, and diplomatic efforts to host major scientific meetings and conferences in critical and emerging technology areas.

The PRC's R&D and manufacturing priorities include its intent to be the world-leading developer in areas such as:

- Artificial intelligence
- Quantum information sciences
- Semiconductors
- New materials
- Smart manufacturing and robotics
- Brain science
- Genetics and biotechnology
- Deep space exploration

You will note many similarities if you compare their list to prior and current U.S. Critical and Emerging Technologies lists.

Every developing and developed economy pumps funding into R&D, pursues global partnerships, and seeks to trade in high-tech goods. What distinguishes the PRC is its use of illicit as well as licit means to acquire foreign technologies, its engagement in unfair competition in targeted industries, its mandatory strategy of military-civil fusion, and a general lack of transparency.

To face down this challenge, President Biden has taken unprecedented action.

To protect national security, this Administration has levied record fines for export control violations, established new export controls on semiconductors, and expanded controls on outbound investment from the U.S. in certain sensitive technologies and products. We are rebuilding America's lead in semiconductors with the bipartisan CHIPS and Science Act. The Department of Justice has pursued numerous cases related to trade secret theft and economic espionage. These actions are oriented toward industry, the source of high-tech products and significant technology development.

To address risks to research security, the Administration is implementing National Security Presidential Memorandum 33 (NSPM-33) and provisions of the CHIPS and Science Act. Here, the purpose is to make sure that universities and other academic institutions understand the altered global landscape and fulfill their responsibilities as the first line of defense against illicit activity. Unlike proprietary R&D, most academic research is intended for publication and thrives in a global exchange of ideas. But some

research can lie close to applications with national security implications. Access to data can lead to unauthorized transfer and use. The PRC has funded hidden parallel labs to replicate research. And as the PRC learns to conduct better and better leading-edge research, it is unfortunately the case that it will use some of that work to America's detriment.

Members of the academic research community are still catching up to the changes in geopolitics. Many of the things that researchers were encouraged to do only a decade ago, like help establish laboratories in the PRC, are now being discouraged. This is why we must be abundantly clear with the research community about the ways that the PRC and the Chinese Communist Party have changed; how the PRC's policies and practices differ from U.S. industrial and defense R&D efforts; and the ways in which some research activities in the PRC take and exploit U.S. data or technologies to contribute to human rights abuses, the Ministry of State Security's surveillance apparatus, and military aggression. It is essential that we address these issues.

The accompanying increase in scrutiny of U.S. researchers' ties to the PRC has given rise to another essential issue. For many Asians and Asian Americans, research security efforts run the risk of exacerbating anti-Asian sentiment, which had already increased during the COVID-19 pandemic. That is why the Biden-Harris Administration has been clear that we cannot and will not pursue policies or processes that worsen xenophobia.

In addition, as captured in NSPM-33, "the open and collaborative nature of the United States R&D enterprise underpins America's innovation, S&T leadership, economic competitiveness, and national security." It is crucial that we maintain that open and collaborative environment to compete effectively in the global race for science and technology.

We are implementing research security with these things in mind, along with our partners in the National Security Council, the Office of Management and Budget (OMB), and the members of the National Science and Technology Council Subcommittee on Research Security. This includes the release of NSPM-33 implementation guidance in 2022, which consisted of multiple rounds of public consultation with outside stakeholders, research organizations, and members of the Asian-American community.

Late last year, OMB finalized and the National Science Foundation posted common disclosure forms for use by all agencies as developed by the National Science and Technology Council and required by NSPM-33. This month, OSTP released guidance on the use of these common forms to provide additional clarity to researchers, research institutions, and agencies on how they can use the information disclosed in the forms to make informed decisions about research funding and performance. The forms also make clear that federally funded researchers cannot be members of malign foreign talent recruitment programs, as required by the CHIPS and Science Act of 2022. In addition, these forms help reduce the overall reporting burden for recipients of federal funds by having clear and consistent requirements across government agencies.

We are completing work on the research security programs requirement after receiving extensive public comments on a draft published in the Federal Register in March 2023. These requirements for research security programs at universities will provide clear standards on research security training, cybersecurity, export control training, and foreign travel security. It is vital that these programs be more than a checkbox—that they achieve increased awareness of research security threats and enable researchers and academic institutions to respond appropriately.

Additionally, we have released guidelines on foreign talent recruitment programs, as required by the CHIPS and Science Act of 2022. These guidelines intend to limit conflicts of interest with foreign governments for federally funded researchers, while not disrupting the United States' ability to engage in productive scientific exchanges that are in the national interest.

In all of these situations, it is our responsibility as the government to establish clear lines about what is and is not acceptable so that our scientists and engineers can focus on delivering the progress that will maintain America's leading position.

There is no question that the PRC is a formidable actor in technology and R&D, with rapid growth, funding, focused efforts, and efforts to systematically collect information that could give it a strategic advantage. American R&D is still strong, but we are no longer the sole big player on the world stage, and we can't rest on our laurels.

The bipartisan support of this committee has helped ensure the United States' strong position in R&D across decades. I want to thank you for that consistent dedication. It has shaped the lives of Americans in every part of our Nation, creating jobs, improving health, changing how we connect and live and work, and making every one of us safer and more secure. We must get today's R&D right so that science and technology can continue to help create a better future.

Thank you, and I will be happy to hear your thoughts and questions.

Arati Prabhakar, Ph.D., is Director of the White House Office of Science and Technology Policy (OSTP) and Assistant to the President for Science and Technology. In this capacity, Prabhakar is the President's Chief Advisor for Science and Technology, a member of the President's Cabinet, and co-chair of the President's Council of Advisors on Science and Technology (PCAST).

An engineer and applied physicist with broad management and leadership experience, Prabhakar has led two different federal R&D agencies and worked with startups, large companies, universities, government labs, and nonprofits across a wide variety of sectors to create new solutions for critical challenges. She served as director of DARPA, the Defense Advanced Research Projects Agency, from 2012 to 2017. In 1993, she was confirmed by the U.S. Senate as director of the National Institute of Standards and Technology (NIST), becoming the first woman to lead the agency. Between these federal leadership roles, Prabhakar spent 15 years in Silicon Valley as a company executive and as a venture capitalist. In 2019, she founded Actuate, a nonprofit organization to develop new approaches to innovation for society's essential challenges.

Prabhakar's family immigrated from India to the United States when she was three years old, moving first to Chicago and then Lubbock, Texas, where she went on to earn an electrical engineering degree from Texas Tech University. She also earned an M.S. in electrical engineering and a Ph.D. in applied physics from the California Institute of Technology. She started her career in the legislative branch as a Congressional Fellow at the Office of Technology Assessment.

She is a fellow of the Institute of Electrical and Electronics Engineers and a member of the National Academy of Engineering, and was a fellow at the Center for Advanced Study in the Behavioral Sciences at Stanford University.

Chairman LUCAS. Thank you, Doctor.
I now recognize Dr. Keiser for 5 minutes to present her testimony.

**TESTIMONY OF DR. REBECCA KEISER,
CHIEF OF RESEARCH SECURITY STRATEGY AND POLICY,
NATIONAL SCIENCE FOUNDATION**

Dr. KEISER. Thank you. Thank you very much, Chairman Lucas. Chairman Lucas, Ranking Member Lofgren, and Members of the Committee, it is a privilege to appear before you today to discuss how NSF is working to secure the Nation's research enterprise, while investing in groundbreaking innovations. When I was doing my homework and reviewing NSF-funded research in your districts, I saw that it ranged from cybersecurity education to advanced manufacturing. And now I see, of course, why other countries covet the U.S. research ecosystem.

At this time of unprecedented global competition and concerning actions by the government of the People's Republic of China, addressing research security is an essential part of meeting NSF's mission, and it's critical to our Nation's economic and national security.

In 2020, acting on the recommendations of national security experts, and thanks to this Committee, NSF created my current position. Over the past 3 1/2 years, the agency has moved quickly to implement many reforms and new requirements to help safeguard the taxpayers' investments in NSF-funded research. In doing so, we've developed a set of basic principles that guide our strategy to research security.

First, we need to be clear, comprehensive, and consistent. NSF is focused on working to develop practical, implementable policies for disclosure and to address research security risks, while minimizing administrative overhead. In 2019 and 2020, NSF actions included emphasizing compliance with disclosure requirements both for NSF staff and NSF-funded institutions and researchers, barring NSF staff from participating in foreign talent recruitment programs, and requiring annual security training for all NSF employees. In addition, after passage of the *CHIPS and Science Act*, NSF has implemented the prohibition on funding for researchers who participate in malign foreign talent programs.

Now, we need to scale research security efforts to the risk, and we're identifying and addressing issues that may be unique or more prevalent in particular areas of research. To be vigilant, we've developed a keen focus on data and analysis. It's been critical for NSF to develop and fund capabilities to better understand the scope and the scale of research security issues and potential breaches.

NSF's system uses open-source data and allows the agency to assess whether affiliations, sources of funding, patents, collaborators, company ownership, et cetera, have been reported properly. It further analyzes author affiliations, clusters, proposals, and awards by topic, researcher, and country, and identifies inconsistencies in materials submitted by researchers. Importantly, these analytical tools can identify participation in malign foreign talent programs, even when that participation is not disclosed.

However, we need to get beyond compliance and develop robust education and outreach efforts to transition from a culture of compliance to one of partnership. NSF and our partners have focused intensively on reaching out to the academic community to build awareness, understanding, and shared commitment. To be successful, we must provide training and tools for researchers. On January 30, NSF launched four interactive online research security training modules that we developed in partnership with our agency counterparts that are available to researchers and institutions across the United States. They provide researchers with clear guidelines, effective strategies to protect against existing and emerging research security threats.

Furthermore, NSF is in the process of establishing the Information Sharing and Analysis Organization called for in the *CHIPS and Science Act*. This center will provide needed information and tools to the research community. NSF is currently reviewing proposals, and we expect to make an award this summer. We're confident that we'll be able to establish an innovative center that strengthens the security of our national research enterprise as envisioned by the law.

And finally, we must also preserve and amplify the value of the research ecosystem. This requires maintaining and actively promoting the values that make the research enterprise successful: openness, transparency, reciprocity, and collaboration. NSF welcomes and encourages international collaboration with likeminded partners. It's essential to pursue the frontiers of science.

Thank you very much for this opportunity to testify before you today, and I'm happy to answer any questions that you may have.

[The prepared statement of Dr. Keiser follows:]



Dr. Rebecca Keiser
Chief of Research Security, Strategy, and Policy
U.S. National Science Foundation
Before the
Committee on Science, Space, and Technology
United States House of Representatives
“Examining Federal Science Agency Actions to
Secure the U.S. Science and Technology Enterprise”
February 15, 2024

Chairman Lucas, Ranking Member Lofgren, and Members of the Committee, my name is Dr. Rebecca Keiser, and I am the Chief Officer for Research Security, Strategy, and Policy at the U.S. National Science Foundation. It is a privilege to appear before you today to discuss how the National Science Foundation is working to secure the nation's research enterprise and protect the taxpayer investments that are critical to advancements in science, technology, engineering, and mathematics (STEM), and STEM education research while promoting principled international research collaborations.

Established by the National Science Foundation Act of 1950 (P.L. 81-507), the U.S. National Science Foundation (NSF) is an independent federal agency charged with the mission "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes." NSF is unique in carrying out its mission by supporting research across all fields of STEM, and at all levels and settings of STEM education.

At this time of intense global competition, securing the nation's research enterprise is an essential part of meeting the agency's mission, and it is essential to our nation's economic and national security. NSF works closely on this effort with our agency counterparts, including the Departments of Energy and Defense, the National Institutes of Health (NIH), and the federal law enforcement and intelligence communities. The agency does so while emphasizing the importance of balancing research security with international collaboration and the nation's ability to attract and retain global talent. NSF has worked quickly to address an age of new threats and challenges, dedicating considerable effort and resources to raise awareness of these threats and to implement needed

requirements, training, and oversight. NSF's efforts have led to ongoing initiatives aimed at clarifying proposal preparation and award administration requirements, as well as the issuance of new policies and directives in the proposal and award process. The agency has also focused on providing tools and assistance to the U.S. research community as we have a shared responsibility to safeguard our research enterprise. The agency has developed training modules for both federal and academic personnel and built new analytic capabilities to help us monitor vulnerabilities.

NSF appreciates the leadership of Congress and this Committee in addressing this challenge, and the agency has moved swiftly to implement applicable requirements of the CHIPS and Science Act of 2022 (P.L. 117-167), and the FY 2020 and FY 2021 National Defense Authorization Acts.

Overview of Research Security

In 2019, NSF commissioned a report by the JASONs, a group of U.S. scientists who are uniquely qualified to conduct studies in security matters for the federal government and who possess a strong connection to the research enterprise. The findings of that report and its recommendations have been invaluable to NSF's approach to research security. The JASON report underscored the contributions and critical role that foreign-born scientists and engineers training and working in the United States have made to the nation's preeminence in science, engineering, and technology today. Their recommendations left no ambiguity that the U.S. should maintain a leading position to attract and retain the best global science and engineering talent. However, the JASON report also found that a small group of governments – notably the People's Republic of China – were attempting to benefit from the global research ecosystem without upholding the core values of openness, transparency, and reciprocal collaboration.

In 2019, the United States Government acted by standing up the National Science and Technology Council (NSTC) Research Security Subcommittee. The purpose of the Subcommittee is to coordinate Federal Government efforts to enhance the security and integrity of America's science and technology research enterprise without compromising American values or the openness, transparency, and reciprocity, which must be upheld for the research and innovation ecosystem to flourish. The Subcommittee includes subject matter experts from 18 departments, agencies, and offices in the Executive Office of the President. These experts identified critical emerging technology subfields, which their home organizations determined may be critical to U.S. national security. NSF co-chairs this Subcommittee with the White House Office of Science and Technology Policy (OSTP), the Department of Energy (DOE), and the NIH. In that role, NSF has helped lead the implementation of National Security Presidential Memorandum 33 (NSPM-33), which put in place new standards and requirement to uphold U.S. values in the research enterprise.

In 2020, NSF created a Chief of Research Security, Strategy and Policy (CRSSP) position – the position I currently hold. This position was codified in the CHIPS and Science Act of 2022, which also called on NSF to create an Office of the Chief of Research Security, Strategy and Policy (OCRSSP). The OCRSSP leads NSF's efforts to safeguard the research enterprise, developing policies and guardrails that balance the security of federally funded research with initiatives that maintain an open and collaborative international research environment; collaborates with federal partners and the White House to coordinate efforts aimed at improving research security and integrity at the federal level; and engages with international partners to ensure current and future international collaborations continue to abide by our core values.

Federally funded organizations also have a role as stewards of that research. Organizations receiving federal funding must demonstrate robust leadership and oversight; establish and administer policies to promote transparency and guard against conflicts of interest and commitment; provide training and information on research security; ensure effective mechanisms for compliance with organizational policies; and implement processes to assess and manage potential risks associated with foreign collaborations and data. Ultimately, research security is about protecting American competitiveness. Ethical behavior is foundational to the conduct of research, and it can only be achieved when everyone can collaborate in an open environment, shielded from the threats of dishonest and unethical behavior that can be caused by undue foreign influence.

Safeguarding Taxpayer Investments

The future of U.S. competitiveness requires that we safeguard critical investments and take steps to address research security while also cultivating vibrant international partnerships that are critical to success. NSF plays a leading role in federal efforts to address research security and is expanding capabilities and competencies to protect the U.S. science and engineering enterprise.

Prior to NSPM-33 and the CHIPS and Science Act, NSF was already working diligently to put measures in place that strengthen research security and integrity for the NSF-funded research community and for NSF staff. In 2019 and 2020, NSF actions included emphasizing compliance with disclosure requirements in NSF's Proposal and Award Policies and Procedures Guide¹ for NSF staff and NSF-funded institutions and researchers; requiring all NSF personnel to be a U.S. citizen or in the process of becoming a citizen; barring NSF staff from participating in foreign talent recruitment programs; and, requiring an annual "Science and Security Training" for all NSF employees.

In January 2022, the National Science and Technology Council's Research Security Subcommittee issued implementation guidance for NSPM-33. A key effort in the Implementation Guidance was the harmonization of disclosure requirements across the Federal government for those applying for research and development funding. NSF and NIH stewarded these harmonized disclosure forms and they have been approved by OMB and are now in effect, adding transparency and consistency in the federal funding process.

Over the past year, with the increased funding the agency received in the FY 2023 Omnibus Appropriations Act, NSF has moved swiftly and made significant progress in implementing Research Security provisions contained in the CHIPS and Science Act. NSF implemented the prohibition on funding for researchers that participate in a malign foreign talent program, as defined in the CHIPS and Science Act. Research institutions must certify to NSF that they have a program to identify malign foreign talent recruitment program members through the proposal and annual reporting process. In addition, the senior personnel on an NSF proposal who are responsible for the design and conduct of the research must certify they are not part of such a program, and they must do so annually during the term of an NSF award. Malign foreign talent recruitment programs include any program in a country of concern.

¹ <https://new.nsf.gov/policies/pappg/23-1/summary-changes>

Consistent with the agency's published System of Records Notice² NSF has also established new analytic capabilities to proactively identify conflicts of commitment, vulnerabilities of pre-publication research, and risks to the merit review system. In 2023, NSF published³ how it approaches these practices. The guidelines include a breakdown of which agency personnel may conduct research security-related activities; what activities to monitor proposal and award disclosures are allowed and with what resources they are conducted; how information will be validated to ensure accuracy; and how information may be shared within NSF and externally. As directed by the CHIPS and Science Act, NSF will scale up the use of these analytics and contribute to NSF's Small Business Innovation Research due diligence process in FY 2024.

NSF is in the process of establishing the Research Security and Integrity Information Sharing and Analysis Organization called for in the CHIPS and Science Act. Called SECURE, this center will provide needed information and tools to the research community. Full proposals for SECURE were due at the end of October 2023, and NSF is currently reviewing those proposals and we expect to make an award this summer. NSF is confident that we will be able to establish an innovative center that will build the capacity of the research community to make risk-informed decisions and create a trusted partnership on research security between research-awarding agencies and the research community, thus strengthening the security of our national research enterprise as envisioned by the law.

NSF, in partnership with the interagency community, including the Departments of Defense and Energy, and the NIH, developed research security training modules for the research community. On January 30th, NSF launched four interactive online research security training modules, now available to researchers and institutions across the U.S. These modules are designed to facilitate principled international collaboration in an open, transparent and secure environment that safeguards the nation's research ecosystem. These training modules signify a major first step in reconciling the needs of the research, law enforcement, and intelligence communities to pursue trusted relationships in the global research community while minimizing economic and security risks. They provide researchers with clear guidelines and effective strategies to protect against existing and emerging research security threats.

Furthermore, NSF has launched a new program specifically designed to study the field of research security, following the federal requirements outlined in NSPM-33 and its accompanying implementation guidelines. The Research on Research Security Program will help us understand the full nature, scope, challenges, and potential of this important field and its critical areas, including cybersecurity, foreign travel security, research security training, and export control training. The program will specifically fund projects that assess the methods for identifying research security risks and the strategies for preventing and mitigating them. Along with raising awareness for the field, this research will inform the development of best practices for research communities, offering guidance to researchers on how to protect their work, enhance transparency and collaboration, and responsibly disclose research findings and other proactive steps to ensure the integrity of our nation's research model. There is significant international partner interest in this research program and NSF will hold a workshop this spring.

² <https://www.federalregister.gov/documents/2021/11/09/2021-24487/privacy-act-of-1974-system-of-records>

³ <https://new.nsf.gov/research-security/guidelines>

NSF coordinates its activities with OSTP, DOE, NIH, and other departments and agencies, including the Department of Justice and members of the Intelligence Community. In addition, NSF works very closely with its Office of the Inspector General (OIG), an independent oversight office that reports directly to the National Science Board and Congress. The OIG is responsible for conducting audits, reviews, and investigations of NSF programs, and of organizations and individuals that apply for or receive NSF funding. This responsibility includes auditing awardees to ensure that they maintain an appropriate conflict of interest policy for employees consistent with NSF requirements. The OIG also conducts financial audits and investigations to determine whether awardees are misusing taxpayer funds; failing to report financial support; duplicating research; and violating rules, regulations, or policy, including allegations of research misconduct (e.g., falsification, fabrication, and plagiarism). NSF has taken, and will continue to take, swift action, such as terminating grants and debarring researchers when the OIG reports incidents to NSF and such action is appropriate. NSF partnered with the Office of the Director of National Intelligence to develop the Safeguarding Science Toolkit⁴, an online resource for the community with information about research security and sensitive technology areas. And NSF is a member of the National Counterintelligence Task Force (NCITF) so that our agency can coordinate with both other civilian and DoD science agency partners and the intelligence community through NCITF on research security issues.

Conclusion

Safeguarding taxpayer investments in research and innovation is central to the nation's global leadership in STEM. NSF welcomes and encourages international collaboration with like-minded partners and views it as essential to pursuing the frontiers of science. Along with our federal partners, NSF has engaged in robust discussions with international colleagues bilaterally, as well as through groups like the G7, to develop common frameworks for understanding and addressing research security. The research community, industry, individual researchers, and the U.S. Government must work together to identify, understand, and address the risks posed to the research ecosystem by foreign actors that do not share those values; improve awareness of these risks through increased communication and information sharing; and promote practices that further the principled conduct of research. This partnership must strike a balance that safeguards the security and integrity of current and future independent and collaborative scientific efforts; conducts appropriate risk assessments that ensure the research enterprise continues to operate with the highest integrity; and ensures U.S.-based researchers and research organizations have the tools and support they need to continue the world-class innovation that has made the American research enterprise a leading contributor to our nation's economic and national security.

NSF's collaborative, well-established relationships with our federal partners, the law enforcement and intelligence communities, and with the NSF OIG have been critical to our response to threats to NSF-funded research from foreign interference. In addition, Congress's actions, including through the CHIPS and Science Act, have provided the agency with necessary authorities and tools to identify and mitigate risks and to put strong requirements in place. As good stewards of American taxpayer funds, we stand ready to take immediate action to safeguard these investments

⁴ <https://www.dni.gov/index.php/safeguarding-science>

when we see new threats arise and we look forward to continuing to work with you on this vitally important issue.

Thank you for the opportunity to testify before you today. I look forward to answering any questions you may have.



Rebecca Spyke Keiser, Ph.D.
 Chief of Research Security Strategy and Policy
 National Science Foundation

Dr. Rebecca Spyke Keiser is the Chief of Research Security Strategy and Policy (CRSSP) at the National Science Foundation (NSF).

Keiser is the first CRSSP, a position established in March 2020 to ensure the security of federally funded research while maintaining open international collaboration. In this role, Keiser provides the NSF director with policy advice on all aspects of research security strategy. She also leads NSF's efforts to develop and implement efforts to improve research security and the agency's coordination with other federal agencies and the White House.

Until March 2020, Keiser was the head of the Office of International Science & Engineering (OISE) at NSF. Keiser had served as head of OISE since coming to NSF in 2015. The office promotes an integrated, international strategy and manages internally focused programs that are innovative, catalytic and responsive to a broad range of NSF and national interests.

Prior to NSF, she was a special advisor to the National Aeronautics and Space Administration (NASA) administrator and an executive-in-residence at American University. She held several positions with NASA, including associate deputy administrator for strategy and policy, associate deputy administrator for policy integration, and executive officer to the deputy administrator.

Keiser also served as assistant to the director for international relations at the White House Office of Science and Technology Policy, where she provided policy guidance to the president's science advisor. Her experience covers science and technology policy, agreements and other cooperative efforts. She is a board member of Women in Aerospace and a member of the American Academy for the Advancement of Science. She has a bachelor's degree in Japanese studies from Wellesley College; a master's degree in politics of the world economy from the London School of Economics; and a doctorate in international studies from the University of South Carolina. She speaks Japanese and Spanish.

Chairman LUCAS. Thank you, Doctor.
I now recognize Dr. Richmond for 5 minutes to present her testimony.

**TESTIMONY OF DR. GERI RICHMOND,
UNDER SECRETARY FOR SCIENCE AND INNOVATION,
DEPARTMENT OF ENERGY**

Dr. RICHMOND. Great, thank you. Thank you, Chairman Lucas, Ranking Member Lofgren, and distinguished Members of the Committee. Thank you for the opportunity to provide an update on the Department of Energy's approach to research security. We appreciate the Committee's sustained efforts to understand this important topic and also develop constructive policies. We also appreciate the close collaboration that we have with our other agencies who are here.

Research security has been a priority for the Department of Energy for decades, dating back to the Manhattan Project. It is enshrined in our mission to ensure America's security and prosperity by addressing its energy, environmental, and nuclear challenges through its transformative science and technology solutions. And what a broad mission that is, from nuclear security to openly conducted basic science in the Office of Science, from funding projects at the 17 national laboratories to supporting research universities all across the country, and more recently to funding development and deployment of those discoveries while building the science and technology workforce. The DOE's mission is critical to our national security and economic security.

In my nearly 50-year career in research in the physical sciences, I personally have witnessed the gradual and now increasingly difficult task of balancing the benefit of open science enterprise and the risks associated with countries of concern, international collaborations, meetings, and contracts in emerging technologies that have the potential national and economic competitive implications that are requiring more careful analysis to ensure that the risks are not compromising the benefits.

We're in a different world today, as you recognize. We're increasingly intense and actions of malign foreign governments pose unacceptable risks to the Nation and to the Department of Energy specifically. It is time, a time when we are pushing the frontier of new technology advances, and success hinges on our Nation's ability to recruit the best and the brightest scientists and engineers in the world.

The Department of Energy takes these threats to our research security very seriously. We take a comprehensive and robust approach to guard against undue foreign influence, which is responsive to changing legislative requirements. Because of the very broad DOE research portfolio, we've expanded our definition of research security to research, technology, economic, security, or RTES, which addresses risk mitigations for each of these research categories.

So DOE has taken three major actions to address the many forms of RTES risks. First, DOE enhanced its existing process to ensure that risks of undue foreign influence are considered early in the competitive process and throughout the lifecycle of a supported

project or loan. Specifically, no person participating in a foreign talent project sponsored by a country of concern may participate in a project. Applications must be fully—applicants must be fully transparent with respect to foreign connections associated with proposed participants, both individuals and entities.

Second, the Department has established a new RTES office, which will implement and continuously refine DOE's process for financial assistance and loan projects, build awareness internally within DOE on RTES issues, engage with external stakeholders, and assist in the review of DOE national laboratory agreements with—involving foreign entities.

And third, DOE has established a departmentwide working group that reports to the Secretary's office to address RTES issues. The group is focused on developing and updating RTES policies. DOE has also established RTES risk mitigation policies designed to protect our national laboratories. Of particular note is the science and technology risk matrix developed in partnership with the laboratories that is designed to protect the most critical emerging research and technologies. The matrix highlights economic and international competitiveness concerns beyond existing controls associated with national security on export controls. National laboratories use this risk matrix every day. To assess international transactions, including requests for foreign national access to our laboratories, staff travel to countries of concern on restricted topics and engagement requests from countries of concern with national laboratories.

So thank you. Thank you to this Committee for highlighting in *CHIPS and Science* how tools such as the science and technology risk matrix are important to our work to address research security. The Department strives to strike the right balance between protecting what has been determined to be most important to DOE and the Nation, while also ensuring our policies do not negatively impact our research ecosystem. This is a process that requires continuing refinement as the world changes, coupled with close dialog with other national laboratories, university partners, and of course, all of you.

So thank you for the opportunity to testify today. I look forward to answering your questions on these important topics.

[The prepared statement of Dr. Richmond follows:]

**TESTIMONY OF DR. GERALDINE RICHMOND,
UNDER SECRETARY FOR SCIENCE AND INNOVATION
U.S. DEPARTMENT OF ENERGY
BEFORE THE
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES
REGARDING
EXAMINING FEDERAL SCIENCE AGENCY ACTIONS TO SECURE THE U.S.
SCIENCE AND TECHNOLOGY ENTERPRISE
FEBRUARY 15, 2024**

Introduction

Chairman Lucas, Ranking Member Lofgren, and distinguished Members of the Committee, thank you for this opportunity to provide an update on the Department of Energy's (DOE or Department) approach to research security. Research security has been a priority for the Department for decades, with policy questions that date back to the Atomic Energy Commission and the secrecy associated with the Manhattan project. We are constantly working to reevaluate and refine our approach to balance scientific collaboration with economic and national security concerns effectively. The Department appreciates the Committee's sustained and purposeful efforts to understand this important topic and develop constructive policies.

Research, Technology, and Economic Security

The Department takes seriously its responsibilities to manage federal funding to the benefit of the taxpayer. We engage in the necessary due diligence and oversight mechanisms to ensure integrity in our programs and to be responsible stewards of the taxpayer dollar. With the enactment of BIL and IRA, which provided more than \$62 billion for programs under the purview of the Department of Energy, it has become more important than ever for the Department to have a comprehensive and rigorous approach to research, technology, and economic security (RTES) policy and procedures for its financial assistance awards and loans. DOE developed, and continues to improve upon, a number of RTES measures to mitigate risk that malign foreign governments pose to our scientific and technological development ecosystem, supply chains, and intellectual property.

To ensure a robust RTES approach, DOE took three major actions to address the many forms of RTES risks. First, DOE enhanced its existing due diligence processes to ensure that risks of undue foreign influence are considered early in the competitive process and throughout the life

of a DOE supported project or loan. DOE also included strict RTES requirements for its financial assistance and loan programs. For example,

- No person participating in foreign talent program sponsored by a country of risk may participate in a project.
- Entities applying for funding must be fully transparent regarding foreign connections associated with individuals and entities proposed to participate in the project. Transparency includes sharing sources of intellectual property, foreign collaborations related to the project scope, foreign ownership, and foreign affiliations. Continued transparency is required during the life of a project.

Second, DOE established a department-wide RTES Policy working group to review, develop, and assist in the implementation of RTES policies. Third, the Department established a new RTES Office to implement and continue to evolve DOE's enhanced due diligence process for financial assistance and loan projects, build awareness internally within DOE on RTES issues, engage with external stakeholders, and review DOE national lab agreements involving foreign entities.

RTES Due Diligence Process

For grants and cooperative agreements, the RTES review occurs at three primary phases in the program lifecycle:

- **Phase 1:** A review is conducted on Funding Opportunity Announcements (FOAs) prior to publication. This ensures that appropriate language is included in the published document, such that potential applicants understand the RTES-related requirements and/or reviews their projects will be subject to.
- **Phase 2:** Prior to selection, a review is conducted of applications that are more likely to be considered for selection.
- **Phase 3:** For funded projects, an RTES review may be triggered in situations where there are changes to the project, personnel, or ownership/control changes that could affect RTES.

A key aspect of the Department's due diligence process is recognizing that addressing RTES risks is the responsibility of the entire Department, not a single office. While the RTES Office serves a central resource to support the program offices in addressing RTES, part of the RTES Office's mission is also to build awareness internally within DOE. Doing so leverages the resources across DOE to identify potential RTES concerns and does not isolate the responsibility to a single office. We want to ensure that each DOE project team of technology managers, project officers, and contracting officers are equipped to understand the RTES concerns, to identify potential concerns as they carry out their merit reviews, review award packages, and monitor ongoing projects. The enhanced due diligence process also relies on the support of the Office of Intelligence and Counterintelligence, DOE's CFIUS Office, and business intelligence tools.

DOE Principles for Evaluating RTES Risk

The following principles guide DOE's decision-making when evaluating RTES risks.

1. **Onshore, Reshore, and Reassert U.S. Leadership in Manufacturing and Deployment of Critical and Emerging Energy Technologies.** The United States must strengthen its competitive edge by making critical domestic investments, especially in sectors that are vital to U.S. national security and economic interests; and protecting and building the resiliency of those investments. Bringing manufacturing back to the U.S. will necessarily involve interaction with foreign entities, but doing so smartly and with eyes-wide-open will ultimately benefit the U.S. economy by developing domestic expertise and building resilient supply chains.
2. **Bolster Supply Chain Security.** Diverse and resilient energy supply chains are imperative for U.S. national security. DOE will support projects that have the potential to build secure supply chains in partnership with our allies and to reduce our reliance on countries of concern. Until we have guaranteed access to secure supply chains, we must remain vigilant that the supply chains we depend on are not exploited by countries of concern.
3. **Make Risk-Based Investment Decisions.** In making historic investments in clean energy, the Department must make risk-based decisions that minimize potential intellectual property loss, supply chain dependencies, and threats to national security. DOE will balance the need to address RTES with the imperative to bolster our overall competitiveness and to maintain core scientific principles of openness and collaboration.
4. **Protect the Taxpayer.** The Department's fundamental responsibility is to be an effective steward and protector of taxpayers' money. If the Department partners with an entity with ties to a country of concern, it will do so in a responsible manner, and only if, after careful deliberation, it is determined there is a significant net-benefit to the U.S. and the risks can be sufficiently mitigated.
5. **Ensure Transparency.** Entities applying for DOE support must be fully forthcoming regarding foreign connections associated with individuals and entities participating in a project, particularly connections involving countries of concern. Transparency includes sharing sources of intellectual property rights, equipment, materials, property, and other support. Likewise, DOE's policies will incorporate transparency.

Research Security at National Labs

DOE has developed, in partnership with the national laboratories, a Science and Technology (S&T) Risk Matrix to protect emerging research and technologies.

The S&T Risk Matrix highlights areas of emerging research and technologies and provides guidance to address potential concern associated with economic and/or international competitiveness that does not overlap or supersede existing controls associated with national security or export controls.

The S&T Risk Matrix uses a Red/Yellow/Green categorization format to quantify the risk associated with a given topic and the resulting level of controls that are required, with red assessed as highest area of risk.

The S&T Risk Matrix applies only to the national laboratories and for international transactions that include country of concern foreign national access requests to the laboratories, travel to countries of risk on restricted topics and country of risk engagement requests with the national laboratories.

For technologies or information determined by DOE in the S&T Risk Matrix to be less sensitive and not restricted, where DOE believes the collaboration will result in a net gain to DOE and the U.S. scientific enterprise, DOE promotes collaboration with nationals and entities, including countries such as China. As this Committee very well knows, countries of concern are limited to China, Russia, Iran and North Korea.

Additionally, in 2019, the Department established a policy prohibiting DOE personnel, to include laboratory M&O contractors, from participating in Talent Recruitment Programs sponsored by countries of concern.

In 2020, that policy was expanded to include a restriction of Other Foreign Government Sponsored or Affiliated Activities sponsored by countries of concern. Participation in these activities must be approved by the Secretary of Energy. The scope of covered activities includes the following: employment, in-kind contributions or promises of future employment in the form of grants, awards, funding, scholarships, and appointments.

The purpose of these policies is to specifically address potential Conflict of Interest (COI) and Conflict of Commitment (COC) that China and other countries use to co-opt DOE researchers and thereby undermine U.S. national and economic security. We work to continually evaluate their effectiveness and improve procedures in order to maximize security for sensitive laboratory information while minimizing negative impacts to critical collaborative efforts among the global scientific community. We also seek to ensure that the administrative burden of these policies and programs is manageable and that our policies do not fuel xenophobia or prejudices in any way.

Intellectual Property Developed with DOE Funding

The Department takes its stewardship of taxpayer funded technologies and facilities extremely seriously. Like our groundbreaking scientific and technological solutions, protecting taxpayer funded intellectual property (IP) is, and has always been, part of DOE's DNA. Now under increasing threat of theft and misappropriation in the current hypercompetitive global environment, safeguarding DOE's and our nation's IP assets is indispensable to U.S. technological competitiveness and leadership. Risk-based IP protections for transformative scientific breakthroughs will help maximize our nation's competitive advantages, establish secure and resilient domestic supply chains, and continue to make the United States the most attractive destination for investment in new energy technologies which boost our energy security and independence.

DOE continues to adapt and evolve our IP safeguards as technologies and their associated risks change. The due diligence and vetting efforts spearheaded by the RTES Office and the continued stewardship of the Science and Technology Risk Matrix ensure that IP considerations will continue to be a key factor in risk management decisions across the DOE complex. In addition, after a comprehensive internal review of the IP licensing practices and procedures at our National Laboratories, the Department is currently working closely with our laboratory contractors to apply targeted risk mitigations and monitoring standards, including enhanced DOE oversight, to ensure that licenses to IP owned by our National Laboratory contractors by law benefit the U.S. economy and taxpayers and protect U.S. economic and national security interests. DOE is also in the process of leveraging new authority under the Bipartisan Infrastructure Law to give our R&D partners additional data protection tools to better enable commercialization and help safeguard against potential misappropriation.

In addition, the Department remains fully committed to ensuring that innovation funded in America stays in America. In fact, DOE took administrative action in 2021 to go beyond minimum statutory obligations to require that new breakthrough science and energy technologies funded by the Department are manufactured here in America. This policy provides a strong signal that DOE is committed to ensuring that all technologies funded by the Department are manufactured in America by U.S. industry and labor whenever commercially feasible. Using DOE policy as a blueprint, in July, President Biden signed Executive Order 14104 formalizing the Administration's "Invent it Here, Make it Here" policy to ensure that the President's historic R&D investments in America benefit American workers, communities, and supply chain resilience. We are pleased to be a part of the Administration's initiative to support domestic manufacturing of technologies that are invented using DOE research funding.

Agency and Administration-wide Commitment to Open Science

America's leadership in Science and Technology (S&T) is underpinned by the unique strengths of our open scientific enterprise. As a democratic nation, our ability to maintain scientific and technological standing is dependent on not only preserving, but promoting the openness of our scientific ecosystem. In addition, promoting international collaboration is crucial to maintaining US science and technology competitiveness and leadership capabilities. We are an open society and that is a key driver in what attracts the best scientific talent from across the globe to our country.

However, the actions of certain foreign governments pose unacceptable risks to the DOE enterprise. DOE must manage risks to research security while maintaining an open, collaborative, and world-leading scientific enterprise.

DOE wants to maintain the benefits of open systems, while incorporating research, technology, and economic security provisions into funding decisions as well as continuing to implement policies to protect the national laboratories and protect against abuses. It is important to understand when competitor nations are seeking to exploit our system and establish the appropriate risk mitigations. DOE must implement nuanced and balanced approaches to combat competitor nations from exploiting our open systems.

DOE's Implementation of Research Security Provisions in the 2020 and 2021 NDAA's, the NSPM-33, and CHIPS and Science

The Department is working diligently to adjust and upgrade DOE's current research security posture in response to Congressional direction on research security via various laws such as the *CHIPS and Science Act*, the *National Defense Authorization Acts* of 2020 and 2021, and the *SBIR and STTR Extension Act of 2022*, as well as Presidential directives such as the National Security Presidential Memorandum 33 (NSPM-33). The CHIPS and Science Act was a historic bill designed to revitalize America's scientific research and technological leadership and strengthen America's economic and national security. This Committee was instrumental in the development and passage of the CHIPS and Science Act, authorizing activities at the Department of Energy that we are uniquely positioned to carry out. The Department is pleased that Congress authorized the Science and Technology Risk Matrix in the *CHIPS and Science Act*, an important risk management tool in the Department's research security toolkit.

In addition to the RTES Office, the cross-cutting RTES Policy Working Group will steward and shape the Department's research security policy approach to ensure compliance with Congressional requirements and direction. The Department continues to engage with the National Science and Technology Council (NSTC) Research Security Subcommittee on common disclosure forms for senior/key researchers pursuant to section 223 of the Fiscal Year 2021 NDAA and NSPM-33 to ensure consistency with legal requirements and agency authorities. DOE has initiated an update to its current and pending support for financial assistance guidance and anticipates posting its conflict of interest/conflict of commitment Notice of Proposed Rulemaking for public comment in the near future. The Department has also initiated a review of its directive on Foreign Government Sponsored or Affiliated Activities, including Foreign Government Talent Recruitment Programs, last updated in 2020, which will, in part, ensure compliance with applicable requirements under the CHIPS and Science Act.

Conclusion

Chairman Lucas, Ranking Member Lofgren, and Members of the Committee, thank you again for the opportunity to testify before you today. I look forward to answering your questions.

Biography of
Dr. Geri Richmond
Under Secretary for Science and Innovation



Geraldine (Geri) Richmond is the Under Secretary for Science and Innovation at the Department of Energy (DOE). In this role she oversees DOE's Office of Science, the nation's largest federal sponsor of basic research in the physical sciences, DOE's applied R&D areas of nuclear, fossil, and renewable energy, and energy system integrity, and the DOE national laboratories and their facilities.

She is currently on leave from the University of Oregon where she holds the Presidential Chair in Science and Professor of Chemistry. Richmond's research throughout her career has been on the use of laser-based and computational methods to understand the molecular, adsorption structure and dynamics at liquid surfaces that have relevance to environmental and technological interests.

She is a member of the U.S. National Academy of Sciences and the American Academy of Arts and Sciences and has been honored by numerous awards including the National Medal of Science (2016), the Priestley Medal from the American Chemical Society (2018) and the Linus Pauling Medal Award (2018).

Her service to the nation includes serving two terms as a presidential appointee to the National Science Board (2012-2021) and as the U.S. State Department Science Envoy for the Lower Mekong River Countries (2015-2016). In addition to serving on many other national and international advisory boards, Richmond has been President of the American Association for the Advancement of Science (AAAS) and Sigma Xi, and the Scientific Research Honor Society.

A career-long advocate for underrepresented groups in STEM fields, she is the founding director of a grassroots organization called COACH that has helped over 25,000 women scientists and engineers in career advancement in the U.S. and in dozens of developing countries around the world. A native of Kansas, Richmond received her B.S. in chemistry from Kansas State University and her Ph.D. in physical chemistry at the University of California, Berkeley.

Chairman LUCAS. Thank you, Doctor.
I now recognize Dr. Lauer for 5 minutes to present his testimony.

**TESTIMONY OF DR. MICHAEL LAUER,
DEPUTY DIRECTOR FOR EXTRAMURAL RESEARCH,
NATIONAL INSTITUTE OF HEALTH**

Dr. LAUER. Chair Lucas, Ranking Member Lofgren, and distinguished Members of the Committee, I appreciate the opportunity to appear before you to testify on the work that NIH is doing to protect the integrity of the U.S. biomedical research enterprise from inappropriate foreign interference. It is through these efforts that NIH enables scientific discovery while assuring honesty, transparency, integrity, fair merit-based competition, and protection of intellectual capital and proprietary information. We appreciate the Committee's continued interest and support of our efforts to address research security issues.

As the largest public funder of biomedical research, NIH sets the standard for innovation and scientific discovery. We promote the highest levels of scientific integrity and public accountability in the conduct of science. We promote open collaboration by leveraging formal and informal cooperation of scientists at research institutions around the world. This exchange of knowledge is an essential part of innovation and is critical to our global competitiveness.

Some foreign entities and governments, however, have exploited the openness of our research system in order to obtain a competitive advantage. In 2018, NIH described its observations about certain behaviors, which do not align with our focus on integrity. The description was developed as a response to NIH learning in 2016 about certain inappropriate activities of some peer reviewers who had been involved with foreign talent recruitment programs or other foreign entities.

These behaviors include stealth employment, often at the behest of malign foreign talent recruitment programs; undisclosed and sometimes duplicative sources of foreign research support; undisclosed financial conflicts of interest, sometimes involving tens of thousands or even hundreds of thousands of dollars given directly to scientists in personal bank accounts or even in cash; breaches of peer review integrity rules; and repeated misrepresentations to institutional officials and to NIH. These misrepresentations are sometimes abetted by foreign institutions in the form of what we call comfort letters, which contain demonstrably false information and can only be interpreted as attempts to mislead American universities and U.S. Government agencies.

Since 2018, NIH has received allegations involving over 600 scientists. We in our Office of Extramural Research have contacted institutions in 255 cases where there were likely foreign interference concerns with scientific or budgetary overlap, overcommitment, or undisclosed financial conflicts of interest. Our efforts have led to hundreds of administrative actions on grants, three criminal convictions, and two false-claim civil settlements.

Nonetheless, it is important to keep in mind that fewer than 1 percent of the approximately 40,000 NIH-funded principal investigator scientists have been linked to foreign interference concerns.

Since 2020, the number of new allegations of undue foreign interference have substantially declined and most have come from university self-disclosures. This trend may be related to outreach on the part of government agencies and professional groups. We appreciate the proactive efforts many recipient institutions are taking to comply with longstanding disclosure requirements.

NIH has no tolerance for breaches of integrity or misuse of taxpayer funds. It is never acceptable for scientists or institutions to hide significant financial interests or to provide information that is not true, complete, or accurate, as this behavior may lead our agency to make inappropriate funding decisions. It is particularly concerning when problematic behavior occurs at the instigation of or with the support of malign foreign actors.

We are pleased to work with our colleagues in the White House Office of Science and Technology Policy and the other agencies who are here on implementing NSPM-33. Our work with the NSF, with OSTP, and with our other colleagues here help create updated forms, instructions, and policy terminology for disclosure documents that also aim to reduce administrative burdens. We have also partnered with other agencies and participated in National Academies and international programs.

Thank you for the opportunity to be here today. I look forward to answering your questions.

[The prepared statement of Dr. Lauer follows:]

DEPARTMENT OF HEALTH AND HUMAN SERVICES

NATIONAL INSTITUTES OF HEALTH

Testimony before the House of Representatives Committee on Science, Space and Technology

Examining Federal Science Agency Actions to Secure the U.S. Science and Technology
Enterprise

Michael S. Lauer, M.D.

Deputy Director for Extramural Research

National Institutes of Health

February 15, 2024

Chair Lucas, Ranking Member Lofgren, and distinguished members of the committee, I appreciate the opportunity appear before you to testify on the work the National Institutes of Health (NIH) is doing to protect the integrity of the U.S. biomedical enterprise from inappropriate foreign interference. It is through these efforts that NIH enables scientific discovery while assuring honesty, transparency, integrity, fair merit-based competition, and protection of intellectual capital and proprietary information. We appreciate the Committee's continued interest and support in our efforts to address research security issues facing biomedicine.

The United States is the world leader in biomedical research. As the largest public funder of that research, NIH sets the standard for innovation and scientific discovery that aims to advance the health of the nation. We exemplify and promote the highest levels of scientific integrity, public accountability, and social responsibility in the conduct of science. We promote open collaboration by leveraging the formal and informal cooperation of scientists at research institutions around the world, which is imperative to solving the most pressing and perplexing public health challenges. This exchange of knowledge is an essential part of innovation, and it is critical to our global competitiveness.

The overwhelming majority of researchers participating on NIH grants, whether U.S. or foreign born, are honest, hard-working contributors to the advancement of knowledge that benefits us all. Integrity and international collaboration should be thought of as "both-and" rather than "either-or."

Some foreign entities and governments, however, have historically attempted to exploit the openness of our research system, in order to obtain a competitive advantage.

Ensuring the integrity and academic competitiveness of U.S. biomedical research and innovation is a top priority for NIH. In 2018, NIH developed and published a list of behaviors which do not align with NIH's focus on integrity. The list was developed as a response to NIH learning, in 2016, about certain inappropriate activities of some peer reviewers who had been involved with foreign talent recruitment programs or other foreign entities.

These behaviors can include the following:

- Stealth employment, often at the behest of malign foreign talent recruitment programs;
- Undisclosed and sometimes duplicative sources of foreign research support;
- Undisclosed conflicts of interest, sometimes involving tens of thousands or even hundreds of thousands of dollars directly given to NIH-funded scientists in personal bank accounts or even in cash;
- Breaches of peer review integrity rules; and
- Repeated misrepresentations to institutional officials and to NIH. These misrepresentations are sometimes abetted by foreign institutions in the form of "comfort letters" which contain demonstrably false information and can only be interpreted as attempts to mislead American universities and US government agencies.

As part of its standard policies and processes, NIH requires grant applicants and recipients to attest that information provided to the agency is true, complete, and accurate; furthermore, applicants and recipients attest that the information provided is true to the best knowledge of Principal Investigators. More recently, NIH has added language to its disclosure forms in which Principal Investigators and Key Personnel must personally sign a statement attesting to the truth, completeness, and accuracy of their disclosures. Should NIH learn of possible misrepresentations or violations of grant terms and conditions, it will conduct a review, often in

concert with institutional officials, and as appropriate implement remedies and/or enforcement actions in line with existing regulations. These include, but are not limited to, specific award conditions, funding restrictions, grant suspension or termination, and/or referral to other agencies including the DHHS Office of the Inspector General.

If NIH identifies potential misrepresentations on grant documents or non-compliance with terms and conditions of award, we conduct thorough, rigorous, and in-depth grant reviews, and, as appropriate, we will work with our recipient institutions to help protect the research and the funding itself. If necessary, we will work with institutions to pursue administrative actions that they can take involving specific grants, to have funds returned, to suspend or terminate awards, or to share relevant information with law enforcement as appropriate.

As published on our website ([Foreign Interference | grants.nih.gov](https://www.nih.gov/extramural-research/foreign-interference-grants)), since 2018 NIH has received allegations involving over 600 scientists. We in the Office of Extramural Research have contacted institutions in 255 cases where there were likely foreign interference concerns with scientific or budgetary overlap, overcommitment, or undisclosed financial conflicts of interest. Our efforts have led to hundreds of administrative actions on grants, three criminal convictions, and two false-claims civil settlements. Nonetheless, it is important to keep in mind that fewer than 1% of the approximately 40,000 NIH-funded Principal Investigator scientists have been linked to foreign interference concerns.

Since 2020, the number of new allegations of undue foreign interference have substantially declined, and most have come from self-disclosures on the part of universities discovering problems on their own. This trend may be related to outreach on the part of government agencies and professional groups. We appreciate the proactive efforts many recipient institutions are taking to comply with longstanding disclosure requirements meant to prevent or address just the kinds of behaviors we have seen in our foreign interference cases.

NIH has no tolerance for breaches of integrity or misuse of federal taxpayer funds. It is never acceptable for scientists or institutions to hide significant financial interests or to provide information that is not true, complete, or accurate, as this behavior may lead our agency to make inappropriate funding decisions. It is particularly concerning when problematic behavior occurs at the instigation or support of malign foreign actors.

We were pleased to work with the White House Office of Science and Technology Policy on implementing the National Security Presidential Memorandum 33, a document which describes cross-government efforts to address research security concerns. Our work with the National Science Foundation helped create updated forms, instructions, and policy terminology for disclosure documents that also aim to reduce administrative burdens. We have also partnered with other agencies to develop research security programs, and we participate in related National Academies and international outreach. NIH will continue to diligently protect the security and integrity of U.S.-taxpayer funded biomedical research, along with all of our federal partners.

Thank you for the opportunity to be here today. I look forward to answering your questions.

Biography



Michael Lauer, M.D., is the Deputy Director for Extramural Research at the National Institutes of Health (NIH), where he serves as the principal scientific leader and advisor to the Director of the NIH on all matters relating to the substance, quality, and effectiveness of the NIH extramural research program and administration. He received education and training at Rensselaer Polytechnic Institute, Albany Medical College, Harvard Medical School, Harvard School of Public Health, and the NHLBI's Framingham Heart Study. He spent 14 years at Cleveland Clinic as Professor of Medicine, Epidemiology, and Biostatistics. During his tenure at the Clinic, he led a federally funded internationally renowned clinical epidemiology program that applied big data from large-scale electronic health platforms to questions regarding the diagnosis and management of cardiovascular disease. From 2007 to 2015 he served as a Division Director at the National Heart, Lung, and Blood Institute (NHLBI), where promoted efforts to leverage big data infrastructure to enable high-efficiency population and clinical research and efforts to adopt a research funding culture that reflected data-driven policy. He has received numerous awards including the NIH Equal Employment Opportunity Award of the Year and the Arthur S. Flemming Award for Exceptional Federal Service in recognition of his efforts to grow a culture of learning and accountability.

Chairman LUCAS. Thank you, Doctor. And I want to thank all the witnesses for your insightful testimony.

The Chair now recognizes himself for 5 minutes.

Dr. Prabhakar, as you mention in your testimony, your office published draft guidance on requirements for research security programs at the universities in March of last year. There's been no communication from OSTP on any progress made since then. Could you please elaborate on what has caused the delay and provide an update on when the final guidance will be issued?

Dr. PRABHAKAR. Thank you, Mr. Chairman. I share your focus on this issue. The research security program guidance is the key thing that we now need to get done, and it is the focus of considerable effort in our office and working with our colleagues. What we learned from the feedback from the community and—inside and outside of government, but across the research base from that draft guidance that we put out gave us considerable pause. We heard many comments on many aspects of the draft guidance. They included concerns about administrative burden, as you might expect because a lot of reporting and training requirements were articulated in that draft guidance, a burden of administrative—an administrative burden that, of course, falls even heavier on smaller research institutions. I think that's a factor.

What really has concerned me even more deeply is—what I want to be sure of is that we don't turn this research security program process into a checklist that an administrator signs off on. The purpose is to make sure that researchers understand this altered landscape so that in their ongoing interactions and when they are recruiting students and postdocs, when they're interacting in the global environment, that they have an awareness of what's going on. And until we do that, that research security program isn't really going to work. So that has turned out to be more complex and taking us much longer than I would like, but I want to assure you that it is a priority and a focus for me and my team.

Chairman LUCAS. Let me offer one follow up question along that line. This is an issue that is critically important to the Committee and for so many purposes overall. If you need any additional authorities or directives from Congress to mandate this, please let us know. We want to help facilitate this process as quickly and as effectively as possible.

Dr. PRABHAKAR. Thank you so much, Mr. Chairman. I really appreciate that.

Chairman LUCAS. Dr. Keiser, Congress directed the NSF in the *CHIPS and Science Act* to develop a plan to identify research areas that require access to controlled unclassified or classified information that may pose a greater risk to our S&T enterprise, should they be targeted by our adversaries, of course. Since the passage of *CHIPS and Science Act* in August 2022, what steps has the NSF taken to develop such a plan?

Dr. KEISER. We have developed a draft risk rubric, and we have announced this risk rubric in our 2024 policy guidance documents. The risk rubric is in draft because we're carefully considering the areas in which we need to assess risk according to NSF's mission of funding fundamental research. So this draft has areas of technology and research that might be higher risk. It has a column to

assess undisclosed international affiliations and sources of funding. It has a column to address affiliations with countries of concern. We're in the process now of road-testing this rubric with the JASON group, which is a group of scientists in the community who do work for the national government in areas of science and security. We'll get their feedback, and then we plan to coordinate this risk rubric with the community and then make it transparent and start implementing.

At the same time, we're not waiting before we assess risk in the new directorate, the Technology, Innovation, and Partnerships (TIP) Directorate, because we do see an enhanced risk because this is research that is more use-inspired, translational, and of interest to our adversaries. So we've been working from the TIP Directorate from the start. We have language in the directorate's solicitations requiring research security programs and points of contact for our awardees. And we've been working also—we have a ban on reviewers for those programs participating in foreign talent recruitment programs.

Chairman LUCAS. Ranking Member, indulge me for one more question.

Dr. Prabhakar, this Committee's first hearing of the 118th Congress focused on considerations for developing a National Science and Technology Strategy to—that would ensure a comprehensive whole-of-government approach to research and development and maximizes the return on taxpayer-funded investments. Congress directed the OSTP to develop the strategy a little later than 1 year after the implementation of the Quadrennial Science and Technology Review. This Committee expected the quadrennial review to be completed by December 31, 2023. Can you give us a progress update on the process of developing the review and when you would anticipate its completion?

Dr. PRABHAKAR. The Quadrennial Science and Technology Review is work that's underway with our interagency process. We've made good progress and hope to be able to get that out quite soon.

I want to say I thought those were just really useful and important provisions and taking that broad look at what we're doing and then where we need to go with science and technology is—I think that's core to our mission, and I appreciated the opportunity to provide both of those reports. I look forward to rolling that out soon.

Chairman LUCAS. And I very much appreciate the old adage about haste makes waste, but the sooner the better so that we can respond to it.

With that, I yield back and recognize the Ranking Member for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. I think this hearing is a very useful one. Certainly, we need to be prudent in terms of protecting the integrity of our research enterprise. On the other hand, we don't want to kill our research enterprise. I'm—as I mentioned in my opening statement, we have a very large number of foreign students who have come here. Really, this is the best place to go for science research. In fact, more than half of STEM (science, technology, engineering, and mathematics) advanced degree recipients in the United States are international students, 16 percent of them from China.

So here's the question. I mean, how do we balance our need to attract the smartest people in the world to want to come here, become Americans in most cases, with the need to protect against some bad actors? How do we get that balance? Are we losing in that balance with the efforts that we're making? Dr. Prabhakar, can you address that?

Dr. PRABHAKAR. Thank you so much, Ranking Member Lofgren. You put your finger on what makes this challenge so complex. And, you know, the measures that were described in law and that we are implementing now, I think, are exactly the right place to start. The specific procedures and having a common forum, having the guidance from agencies so that awareness starts growing in the research enterprise I think is an important place to start.

These are the mechanisms, but again, the endpoint, the picture in my head is what success looks like is that, as you go through the education process, as you start into research, as you become an American researcher in one of our universities or research institutions, part of what you understand about the world is how important it is to have these global collaborations, the warm embrace of immigrants who have brought so much to our science and technology enterprise, and that we're no longer naive in the research community and understand that there are malign actors and illicit activities. And simply being aware is the first place to start, and to me, that's the point of all of these mechanisms. I think we've made some progress in raising that awareness, and as we complete our work, that's where we need to get to.

Ms. LOFGREN. Doctor, it took, as we mentioned, longer than we hoped, but we were glad to see the release yesterday of the common disclosure forms in talent recruitment programs, but universities are still seeking guidance for standards for research security programs. When do we expect that guidance to be issued?

Dr. PRABHAKAR. Yes, I—yes, they are looking for that. I know—I hear their frustration, and I share it because I think we've introduced these ideas, but now we actually need to be clear with everyone exactly what they need to implement. So I understand that urgency. We are working through the very significant comments that we received on the draft guidance and revectoring accordingly. That is work that's happening with the interagency process, and it's a significant focus. It's a personal priority for me because I think we need to get this sorted and clear for everyone. We will—we are very much looking forward to getting that rolled out and completed.

Ms. LOFGREN. Drs. Keiser, Lauer, and Richmond, I am interested in what kind of guidance each of you or your institutions are providing to our academic world, awaiting the additional guidance that Dr. Prabhakar just mentioned.

Dr. KEISER. I can start. We, of course, are working very closely with OSTP through the Research Security Subcommittee on this guidance to universities for research security programs. We have worked together as well in releasing the training that I mentioned. And the training is a start. In my view, it is the beginning of this building of this culture of research security so that there's the awareness there. Then, it will build on the next step of having the

standards of how to build an actual research security program itself.

Ms. LOFGREN. So how do we—I mean, I want to hear from the other two doctors, but I'm also concerned that we're not giving conflicting advice between the various agencies, if you can address that as well.

Dr. KEISER. Yes, absolutely. We talk pretty much every day to make sure that we're coordinating on our policies going out to universities. As an example, we mentioned the—this risk rubric effort that I'm dealing with, and I talk to Dr. Richmond's staff frequently about their S&T matrix to make sure that we are consistent in what we're doing for the community. We also work together on the training and the disclosure.

As you said, I think what's key is that we also share information, which is another aspect of NSPM-33 that we'll be working on to develop an information-sharing mechanism among our agencies that protects the privacy of researchers, but still shares information on research security with one another. So we have this informal mechanism, and then through the Subcommittee, we're also working on this more formal mechanism.

Dr. RICHMOND. Well, let me—first of all, that's a really important question, and we certainly are very active with the other agencies to put this together. We've had a disclosure form since 2022 that we have on the web that has a lot of details of what we need because we just—you know, we just have to put things into operation while we wait to get the coordination.

But I would say that even what we have in the disclosure forms now, they're quite consistent with what we're working with other agencies, too, and we're also sharing all the details of our unclassified risk matrix because that is kind of a model that we know to work forward. So I really think that this is—the agency—inter-agency working group is great and NSTC (National Science and Technology Council) working—we've been leadership in that. It's a tough one, but the Department of Energy has had to step out and say we're doing this right now because we've got grants coming in. We've got to do this. We would just like to see more consistency.

Dr. LAUER. I'll just add, I'll echo the comments of my colleagues. We—there's been extensive coordination, but I'll also add that we're trying to send a message that this is not either/or. It's both/and. We can have security and integrity and at the same time have proper collaboration. Proper collaborations do not involve stealth employment, duplicative funding, undisclosed financial conflicts of interest or repeated misrepresentations. And by sending that message in various ways, in many ways, we hope that we can meet exactly on that balance.

I would also say that the fact that we're getting so many self-disclosures and that the majority of our cases now are self-disclosures says something about the effectiveness of the work that everybody here is doing.

Ms. LOFGREN. Thank you, Mr. Chairman, for your indulgence in my going over the time, and I yield back.

Chairman LUCAS. The gentlelady's time has expired.

The Chair turns to the gentleman from Florida, Mr. Posey, for 5 minutes.

Mr. POSEY. Thank you, Chairman Lucas.

Dr. Prabhakar, it's been almost 6 months since the Administration extended the deadline for the U.S.-China agreement on cooperation in science and technology to reportedly allow time to negotiate a new agreement. Does the Administration plan to extend the S&T agreement with China? And if so, what new terms are being negotiated or included?

Dr. PRABHAKAR. Mr. Posey, thank you for your question. That matter of the science and technology agreement is being handled by the State Department, and very much to your point, the purpose of that extension was to consider and to weigh and to negotiate terms, recognizing the reality and the environment that we're currently in. And that matter is under consideration today at the State Department, and so I don't have any more specifics unfortunately.

Mr. POSEY. Yeah, I know. The State Department actually prompted me to file a bill on solar panels. I don't know if you're really familiar with it or not. But one thing President Trump and President Obama agree upon is that we need to have tariffs on China's solar panels. They do them with slave labor, child labor, and they can undercut American products pricewise, obviously, to be noncompetitive. And so the tariffs were a follow-through with both those Administrations. So China started shipping their China-made solar panels through Indonesia, Thailand, and getting a label slapped on them, made in Indonesia and China and avoiding the tariffs. The State Department actually fleshed this out and exposed this, and I filed a bill to reinstate the tariffs, in all fairness to American productivity and passed in the House, passed the Senate, and the President vetoed it.

So I have a little bit of difficulty wondering about the sincerity of putting our country first in these agreements. Can you give me some examples where we've been on the American side and not the Chinese side on some of these issues?

Dr. PRABHAKAR. Mr. Posey, I'm sorry, I'm not familiar with that particular matter. I've referred to several of the actions that this Administration has taken to deal specifically with Chinese industrial espionage, cases that the Department of Justice is pursuing, very strategic thinking about advanced technologies, including artificial intelligence, and what is required in export controls to make sure that we're not simply allowing the PRC to take our most advanced semiconductors, for example, and use them in military systems that we could face in an adversarial situation. That has been the consistent strategy in the work and the thinking across the Administration in dealing with the PRC in this heightened environment.

Mr. POSEY. Thank you for that.

Mr. Chairman, I ask unanimous consent to include in the record that GAO (Government Accountability Office) report, "Research Security: Strengthening Interagency Cooperation Could Help Agencies Safeguard Federal Funding from Foreign Threats."

Chairman LUCAS. Seeing no objection, so ordered.

Mr. POSEY. Thank you, Mr. Chairman. I see my time is about to expire, and I yield back.

Chairman LUCAS. The gentleman's time expired.

The Chair now turns to the gentlelady from Oregon, Ms. Bonamici, for 5 minutes.

Ms. BONAMICI. Thank you. Thank you, Chairman Lucas, Ranking Member Lofgren. Thank you to the witnesses, a special warm welcome to Dr. Richmond, who comes to the Department of Energy via the University of Oregon, glad you're here.

You know, the successful culture of Federal research in the United States relies on open access to scientific information, data, and practices between and among Federal research agencies and academic and research institutions, and often, international partners. I think about all the work that's going on, for example, in northwest Oregon, supercomputing, semiconductors, artificial intelligence, quantum computing. We know that to remain a leader in these fields, we must cultivate a collaborative science ecosystem that preserves integrity without imposing unintended costs on institutions that create a chilling effect on recruiting top scientific talent to the United States.

Leading Federal research institutions—and I think back home about the University of Oregon and Oregon State University—they're taking this issue seriously. They're working to implement necessary compliance measures, creating—they're hiring cybersecurity personnel, reallocating time and funding to manage contracts and comply with training, and creating new administrative departments to meet these security requirements.

So I'm going to start with you, Dr. Prabhakar. You noted that the increased administrative burden and costs are affecting the implementation of the security guidance, so I wonder if you could tell us a little bit more about your work to develop and communicate research security standards, and are research funding agencies providing any resources to institutions to help them alleviate these costs? And would you need dedicated funding to do that?

Dr. PRABHAKAR. Thank you, Representative Bonamici, because this is a practical issue that you're raising and that universities are raising. This is part of what we have to wrestle through as we finalize the research security program guidance. And as that crystallizes, I think we'll be in a much better position to assess what the cost and impact will be to universities. A lot of the complexity is thinking through what it means not just for our premier research universities that have very substantial research funding, but also very substantial administrative structures to be able to handle today's administrative issues. And then, you know, for them, this will be an additional task, but, you know, it'll be an increment to something that they're already geared up to do.

I think about the research universities around the country, HBCUs (historically Black colleges and universities), minority-serving institutions, but across every part of our country we have so much research talent, and we've already been concerned that it's not being unlocked because those smaller institutions don't have the staff to help faculty members write—

Ms. BONAMICI. Exactly right.

Dr. PRABHAKAR [continuing]. Useful proposals. So I think—NSF I think has—and perhaps NIH—I know at NSF there have been really important efforts to make sure we boost that capacity for all of our research institutions that aren't already fully staffed up, and

I think this will then add—the research security measures then will add to that mix.

Ms. BONAMICI. I appreciate that very much.

And, Dr. Richmond, welcome. I want to follow up on Ranking Member Lofgren's line of questioning. You credit U.S. leadership in science and technology research to our open scientific enterprise, which is critical. And you explain that thoughtful international collaboration strengthens our competitiveness and encourages talented researchers to contribute to the cutting-edge work that's being done here. So has the increased suspicion in the name of research security led to reluctance by international partners to engage in Department of Energy-funded research? And also, how—can you talk a little bit about what it looks like to have a research security requirement that doesn't hinder our ability to recruit and retain international talent?

Dr. RICHMOND. Well, thank you very much for that question because—do you mind if I share a story?

Ms. BONAMICI. Please do.

Dr. RICHMOND. I was recently at one of our major universities, and I was talking to a young, sort of midcareer faculty member from China. And he's built a wonderful program there in material science, has a great research group there, and he was almost in tears when he said, I'm scared now. I'm scared that they'll find something in my record that'll make me have to leave, and I'm not involved in any talent program. But it was just—you know, when I think about those that are from other countries, and even some of our own American scientists, that worry that what they've built now is being threatened. And so I hear it. I see it. And so I think that's why it's so important at our universities to develop cultures around them which is about security and also welcoming those that we need to have and the talent.

Ms. BONAMICI. Absolutely. It's critical that we get it right, so I appreciate all your testimony and what you're doing, and I yield back. Thank you, Mr. Chairman.

Chairman LUCAS. The gentlelady yields back.

The Chair now recognizes the gentleman from Texas, Dr. Babin, for 5 minutes.

Mr. BABIN. Thank you, Mr. Chairman, and thank you, witnesses, for being here.

Dr. Prabhakar, last October, FBI (Federal Bureau of Investigation) Director Chris Wray joined the heads of allied foreign law enforcement agencies in highlighting the unique threat the Chinese Communist Party presents to the U.S. scientific enterprise. The quote is, "The People's Republic of China represents the defining thread of this generation, this era. There is no country that presents a broader, more comprehensive threat to our ideas, our innovation, our economic security, and ultimately, our national security. We have seen efforts by the Chinese Government directly or indirectly trying to steal intellectual property, trade secrets, personal data all across the country, and we're talking everything from Fortune 100 companies down to smaller startups. We're talking about agriculture, biotech, healthcare, robotics, aviation, academic research. We probably have somewhere in the order of 2,000 active

investigations that are just related to the Chinese Government's effort to steal information."

Very quickly, do you agree with Chris Wray's assessment?

Dr. PRABHAKAR. Yes, I think it's a good summary——

Mr. BABIN. OK. Yes, ma'am.

Dr. PRABHAKAR [continuing]. Of the situation we're facing.

Mr. BABIN. Thank you. President Reagan back in the 1980's issued National Security Decision Directive 189, which exempted foundational research, both basic and applied, from export controls. Given Director Wray's assessment I just read, do you believe that this exemption should be revisited?

Dr. PRABHAKAR. Thank you for the question. I think it really gets at the heart of what we are grappling with. I want to just take a moment to share a personal reflection. A decade ago, I had returned to public service to lead DARPA (Defense Advanced Research Projects Agency), where I had served many years earlier. When I was the program manager at DARPA, the cold war ended. One day I came to work and there was no longer a Soviet Union. So I saw that chapter of what it meant to try to drive very advanced science and technology in the geopolitics of the late 1980's and early 1990's.

When I returned in 2012, what I found was that the world had changed in a very important set of ways, and the most striking thing was the behavior of the PRC. And that—I think it was starting to become visible in that time period. President Xi, I think, has made a shift that is quite palpable. And what I've seen over the last decade is very much summarized in your remarks, is a PRC that is aggressive. Again, many countries are using technology to try to craft the future, but they are taking it to a place that is causing a different set of problems, and that's very much what we are grappling with——

Mr. BABIN. Absolutely.

Dr. PRABHAKAR [continuing]. In this research in this area.

Mr. BABIN. Well, let me ask this. Does China offer the United States and other foreign nations reciprocal waivers for the export of their foundational research? And if not, why should we maintain this waiver? Do you know the answer to that?

Dr. PRABHAKAR. I'm sorry, I'm not sure the specific issue to which——

Mr. BABIN. OK.

Dr. PRABHAKAR [continuing]. That comment refers.

Mr. BABIN. Does China, does the PRC offer other nations reciprocal waivers?

Dr. PRABHAKAR. I'm so sorry, sir. I don't—I'm not sure exactly what waivers that's in reference to.

Mr. BABIN. Well——

Dr. PRABHAKAR. I'm happy to follow up if that's useful——

Mr. BABIN. Yes, ma'am.

Dr. PRABHAKAR [continuing]. With your staff.

Mr. BABIN. Well, what I'm trying to say is I think they do not offer waivers to the United States and other foreign nations when it comes to their Chinese companies, Chinese researchers, or joint U.S.-China researchers. So my question is, if they don't offer us waivers, why should we offer them waivers? That's my question.

Dr. PRABHAKAR. I'm not familiar with where we might be offering waivers. I think that's what I'm not understanding, so I'm happy to follow up——

Mr. BABIN. OK.

Dr. PRABHAKAR [continuing]. If that's useful. Yes.

Mr. BABIN. OK. One other thing here, I've got a minute left. This is also to you. Yesterday, you released new disclosure guidelines for Federal researchers. As you know, NASA (National Aeronautics and Space Administration) is subject to the Wolf Amendment, which prohibits NASA funding of cooperation with China. A 2022 NASA Inspector General report on NASA insider threats highlighted a number of instances of criminal convictions tied to violations of research security laws and policies related to the Chinese Communist Party. However, one such case that the Department of Justice brought against a University of Tennessee Knoxville professor, who was also a paid professor at the Beijing University of Technology during that summer, was dismissed because of uncertainty about the China funding restriction and vagueness of disclosure guidelines.

Do you believe the new disclosure guidelines that you recently issued will prevent cases like the one I just mentioned where researchers are quote, "unaware," unquote, of restrictions? NASA and the University of Tennessee, Knoxville were very clear, but that didn't seem to matter in the courtroom. So how do these new guidelines ensure greater awareness than what is already required?

Dr. PRABHAKAR. Thank you for that question. That is precisely the purpose of the work that we are doing is to make sure that every researcher is completely clear in this new geopolitics that we are dealing with, and that change is one that many researchers are not yet caught up to. That's exactly why we are doing this work.

Mr. BABIN. Well, we got a fine line to walk here. We don't want to run people off, which has happened in the past, but we also have to protect our information.

Thank you, and I yield back.

Chairman LUCAS. The gentleman's time has expired.

The Chair now recognizes the lady from Michigan for 5 minutes.

Ms. STEVENS. Thank you, Mr. Chair.

Speaking of global challenges and tensions, many of you know that we have a Select Committee on Strategic Competition with the Chinese Communist Party, and it is a bipartisan Select Committee run by Mike Gallagher as the Chair and Raja Krishnamoorthi as the Ranking Member. And the Select Committee issued in December a set of recommendations to bolster the United States and our economic competitiveness, making such recommendations as that we must here in the United States of America fund open peer-reviewed research of critical technologies. And it's important to note that this recommendation was approved in a bipartisan, unanimous fashion.

So to the panel, could you highlight why this recommendation, investing in open research at the levels authorized in *CHIPS and Science* on topics like biotechnology, quantum, and artificial intelligence, is absolutely essential to maintaining our global leadership? And I don't know if Dr. Keiser wants to start or——

Dr. KEISER. Sure.

Ms. STEVENS [continuing]. Ms. Richmond.

Dr. KEISER. Thank you very much for the question. Open research is extremely important, and in my view, we have to communicate very clearly to the community about the concerns in research security, which are not because of openness, but rather they are because other countries are taking advantage of our openness. And I'll tell you what I mean by this. Openness is things like things we're funding in your district such as a global center on climate change, which is collaboration with many other countries, including Canada. We want this data on climate change to be made open so that other researchers can use it, they can challenge it, they can improve on it, and they can continue to innovate. And we can't let adversaries keep us from doing that. That way, they win.

So, at the same time, we need to communicate what issues are we worried about? Well, we're worried about someone coming into the United States or a U.S. researcher taking prepublication research before it's even made open and taking it to an adversarial country to be used for military-civil fusion purposes. That's what we're concerned about. And we have to be very, very clear about that and clear about that distinction.

Ms. STEVENS And, Dr. Prabhakar, just in your role at OSTP, have you—your very important role, by the way—have you observed any of the, you know, maybe potentially chilling effects on scientists when open, collaborative science is demonized, and the impact that that might be having on our economic competitiveness?

Dr. PRABHAKAR. I thought that the Under Secretary's story was telling. And we know researchers have left the United States and returned to China to China's benefit. That happens with friendly countries all around the world, and so some of that could be OK, but we also know that it ultimately is to our economic detriment. And so let's not be driving these people away for sure.

I have certainly heard from the Asian-American and the Asian researcher community about the chilling effect that this whole issue has had. And part of why we have to get these issues resolved is to establish research security and to make sure that that uncertainty is removed and that people can go forth and do the work that we need them to do.

Ms. STEVENS. And you're playing at OSTP such a critical role in keeping scientific research safe, secure, and open. And just with, you know, the minute remaining, could you—just to give you a moment to elaborate on how OSTP coordinates with other Federal agencies to support open, aboveboard scientific research.

Dr. PRABHAKAR. The reason I took this job when the President asked me was because my great passion is science, technology, and innovation for creating the future for our country. And that doesn't happen unless this whole enterprise is robust. And what we're talking about today, research security, is part of making sure it's robust and the environment that we live in. And, as we all know, there is much more. It is funding support. It is making sure that we not only write the best research papers, but that we harness that information and build jobs and industries in every part of the country. It's about meeting our health challenges in this country. It's about dealing with the climate. So that is our everyday work,

and that getting research security right is foundational to achieving all of that.

Ms. STEVENS. And just looking out, right, it is such a treat to have NSF, Department of Energy, and, in unique fashion, the National Institutes of Health here at the Science Committee. And I really want to salute all of you and the agencies you represent, the scientists, and those contributing to this enterprise in the United States of America. So thank you so much, Mr. Chair, and I yield back.

Chairman LUCAS. The gentlelady's time has expired. The Chair now recognizes the gentleman from Tennessee, Mr. Fleischmann, for 5 minutes.

Mr. FLEISCHMANN. Thank you, Mr. Chairman, and thank you for holding this important hearing. To the distinguished panel, thank you very much for your very insightful testimony today. I'm Chuck Fleischmann. I actually represent the Oak Ridge Reservation and all the wonderful things it entails, so I work very closely with the Department of Energy.

I have two questions, so I'm going to ask for a little bit of brevity in response and—but the first one is on standardization. The use of common forms such as biosketch and other support and consistent definitions across agencies are a welcome step for our government, academic, and industry research institutions toward harmonization. Standardization makes it easier for researchers to comply, which in turn safeguards the research enterprise.

My question is how will Federal departments and agencies continue working together to expand on the standardization of definitions and harmonization of procedure?

Dr. PRABHAKAR. I'm happy to start. We put out the common form through the interagency process a few months ago, and then just recently now have put out guidance to agencies to help them make sure that they are getting on the same page about using that. We understand that different agencies have different missions, and there will be times when exceptions are needed, but our current guidance asks that we be informed of that. And I think that—this is the process that will get us to a place that reduces the burden, but actually allows for the transparency that we need.

Mr. FLEISCHMANN. Thank you. Doctor?

Dr. KEISER. Thank you. NSF has implemented the common forms, and I know NIH has as well and Department of Energy, so we're really very much in sync on this. Something now that we have to focus on is communication to the community. No. 1, here's what the common form means, here's how we're using your information, and here's why we need it. And No. 2, we are not interested in going after anyone for making a mistake on the disclosure. This is about making sure that we have all the information that we need to make sound funding decisions and get rid of any concerning conflicts of interest or conflicts of commitment.

Mr. FLEISCHMANN. Thank you.

Dr. RICHMOND. So I would say at the Department of Energy we've done this for a long time with our national laboratories, and so it's not just the information that you gather, but it's also how you use that and how you go back and forth with the institution to get them to figure out what's going on. And so I think there's

a lot—and other agencies have asked us to share the risk matrix which we've released because that helps put together—it's sort of like stoplight, green light, yellow light, red light on what you should go forward with and be cautious about. So——

Mr. FLEISCHMANN. Thank you. Dr. Lauer?

Dr. LAUER. Congressman, I completely agree with your sentiments. I would say that one aspect of this whole experience is that the agencies have been working very closely with one another. Our staff at NIH and the staff at NSF has spent probably thousands of hours working on every last detail of these forms, as well as the research security programs, and that's created a culture of standardization and collaboration and, you know, making things as easy as possible for the research community.

Mr. FLEISCHMANN. Thank you. In my waning moments, the security cost accessibility question, to build upon harmonization across government, we all recognize research security carries additional costs for institutions, such as administrative effort and IT (information technology) system upgrades. How can research security standards be implemented in a manner that allows for more organizations such as small or emerging research institutions to participate?

Dr. KEISER. Thanks. Through the secure center that we are going to be funding, we want to provide assistance, information, tools to all entities, large and small, to help them in the establishment of these research security programs. In fact, my guidance to the team that's currently reviewing these proposals for the center is we want the democratization of research security, and the center needs to help in that regard.

We also are establishing a track through the granted program that Dr. Prabhakar mentioned, which is a program to assist emerging research institutions. And it will be a track in research security as well to help them.

Dr. RICHMOND. And I would say that a number of our national laboratories are providing help with the smaller institutions to provide advice on how to go forward, so I'm really proud of what many of our national laboratories are doing, including Oak Ridge.

Mr. FLEISCHMANN. Thank you.

Dr. LAUER. We're working very closely, of course, with our partner agencies, and we also have a number of efforts underway at NIH to enhance the capacity of research institutions.

Mr. FLEISCHMANN. Thank you. I thank the panel. Mr. Chairman, I yield back.

Chairman LUCAS. The gentleman yields back.

The Chair recognizes the gentleman from Illinois, Mr. Sorensen, for 5 minutes.

Mr. SORENSEN. Thank you, Mr. Chairman and Ranking Member Lofgren, for convening this hearing, and our witnesses for your willingness to appear with us here today.

Openness is a hallmark of the U.S. research ecosystem. Before my career here in Congress, I was a meteorologist by trade, also one of the people that took the risk to start talking about how climate was impacting the weather some 15 years ago. I only did that because I was the trusted communicator of that science. I only did that because I could trust the science that I was learning from.

The purpose of our meeting here today is to protect proprietary technology and scientific discoveries. So I want to continue from what my colleague from Michigan was talking about with Dr. Prabhakar and Dr. Keiser. How can we continue to accelerate the research with respect to climate, while keeping it—and keeping the politics out of it, but keeping the science the focal point?

Dr. PRABHAKAR. Thanks for that question. It's good to see you again, Representative. You know, I'll point to the National Climate Assessment, the Fifth National Climate Assessment that OSTP produced and that the President launched in November of last year, I believe. This is a regular assessment of what is happening with climate change in America. And what that report—this particular report found was something I think Americans across our country see very directly today is that the weather is changing, that the effects of—the many effects of a changing climate on—in terms of intensified storms, in terms of droughts and wildfires. I'm a Californian, and I have dealt with the smoke there many, many times.

That is very visible to everyone, and I think understanding that comprehensively and clearly rolling up that research and making it useful to people so that they can understand what's happening community by community was a lot of the work that we did in that report. We also found that people are taking action across the country, and I found that very heartening because I think this is a problem that—when you're in the middle of a storm, it can feel overwhelming and as if there is no, you know, turnaround in the future.

But in fact, people are taking action across the country with the work that this Congress has done with the *Bipartisan Infrastructure Law*, with the *Inflation Reduction Act*. This Administration has moved out with some of the most significant actions on mitigating climate change. And all of that was—we're starting to see that now in the climate assessment. Everything I just described relies on exactly what you said, which is having a solid base of scientific research, so that continues to be a priority, I know, for everyone here.

Dr. KEISER. And NSF has funded a global center, as you know, for international collaboration in climate change research. And to me, working internationally on our processes, on our research only bolsters the trust in that research itself. And it's related to research security and research integrity. In fact, the U.K. calls their research security effort “trusted research” because if you can build integrity into every step and be transparent about how the research is conducted, you build the trust. And so that's what we're focusing on as well.

Mr. SORENSEN. I appreciate that. I have just about a minute left. I want to go back to you, Dr. Prabhakar. This Committee's Space and Aeronautics Subcommittee, on which I serve as a Ranking Member, held a hearing just yesterday in this room, talking about NASA's plans for decommissioning the International Space Station. The transition will require NASA to go from being the owner and operator of the International Space Station to becoming a customer for one of our commercial space stations. So how might research security policies, practices, and risk postures be different for the Fed-

eral Government, federally funded research as we transition? To what extent is OSTP considering commercial partnerships in developing research security guidance to Federal agencies?

Dr. PRABHAKAR. Thank you for that question. That's a significant transition that NASA is working on, and I appreciate that Subcommittee's focus on such an important issue.

I think as we've been talking about research security here, it's very—the focus here has been the research part, but of course, protecting our technologies is something that is much broader than just the basic research community. And many of the measures that are in place and the actions that have been taken specifically are about protecting our industrial technological capacity.

The space station, though, I think, is a great example of a place where the kind of research happens where there are so many opportunities, and we've had so many excellent international collaborations, so I'm sure that will continue to be a major focus for NASA and its work.

Mr. SORENSEN. And those certainly won't go away.

Mr. Chairman, I yield back.

Chairman LUCAS. The gentleman's time has expired.

The Chair recognizes the gentlelady from New York, Congresswoman Tenney, for 5 minutes.

Ms. TENNEY. Thank you, Mr. Chairman and Ranking Member, and thank you to the witnesses, and thank you for being here and your expertise.

I first wanted to address my question to Dr. Prabhakar. Did I pronounce that right? I would like to just draw attention to your expertise as the Director of the White House Office of Science and Technology Policy and also your previous position as head of the Defense Advanced Research Projects Agency, otherwise known as DARPA. One of the many ways—and you just alluded to this in the last questioner—that we protect sensitive research is through the classification system. And I wanted to ask you a few questions about this process that may seem obvious, but I think it's important for the American people to know since you are dealing with very sensitive information, whether it's China, Russia, or other issues. And I just want to ask you the first question because I'm sure you know the answer to this, but do you know the penalty for willingly retaining or leaking classified information under title 18? It's technically chapter 37 in the U.S. Code.

Dr. PRABHAKAR. Thank you for your focus on this important issue. I have signed a number of documents in the course of my career as I have received security clearances. I don't know the specific penalties, but it was always clear to me that—the legal reasons and the penalties were one of the many reasons that I would not be disclosing classified information, so I know it's a serious—

Ms. TENNEY. The answer—

Dr. PRABHAKAR [continuing]. Very serious—

Ms. TENNEY. And I understand this is technical, but the answer is actually that it's up to 10 years of imprisonment for violation of that section. And so if the proper investigatory process found that this—that an employee, say, under your advisory, someone in the department knowingly and willfully mishandled and disclosed clas-

sified documents repeatedly, would you continue to provide that individual with classified information?

Dr. PRABHAKAR. A serious violation of that sort would obviously require revoking of the clearance and whatever other steps would be required.

Ms. TENNEY. Would you fire someone that did that?

Dr. PRABHAKAR. I have not encountered that circumstance, but when—if allegations of that sort were verified, then of course, there would be legal action, but also employment action I would expect.

Ms. TENNEY. OK. Or at least a leave from the position in the event that that would happen?

Dr. PRABHAKAR. I can't speculate, but of course—

Ms. TENNEY. OK.

Dr. PRABHAKAR [continuing]. It's such a serious matter, it would have to be handled with—it would have to be taken very seriously, obviously.

Ms. TENNEY. Thank you. And I know you're an expert on this, and I'm bringing this up just because it's obviously relevant to everything that's happening. But last week, Special Counsel Robert Hur concluded that President Biden knowingly and willfully removed, mishandled, and disclosed classified documents repeatedly over a period of decades, not just a few years. Special Counsel Hur also found that President Biden's cognitive decline was so severe that he likely could not convince a jury that Biden's actions were not willful. Either President Biden, in my opinion as a lawyer, is mentally competent and must stand trial, or the Cabinet must invoke the 25th Amendment or at least look into proceedings on that to remove him from office. And I'm wondering if that's something that you would consider in light of the bombshell testimony that came out of the Special Counsel's Office.

Dr. PRABHAKAR. Representative Tenney, I can simply say to you that in my interactions with the President in many meetings that—what I have seen is someone who is very focused and digs into details and is very incisive and—

Ms. TENNEY. OK. So if he's very focused and able to do the details, do you feel that he—did he mishandle—I mean, the Special Counsel determined that he mishandled documents, so shouldn't he be able to stand trial on that?

Dr. PRABHAKAR. I'm sorry, I—I'm not in a position to comment on the special prosecutor's report.

Ms. TENNEY. Thank you. I understand. Now, I just want to get into a couple of questions on China since China is such sensitive information. And my concern is—and obviously, in the scientific community that researchers sometimes don't take the—China's threat as seriously as they should. And I was just wondering what the policy was in your office on China, how deeply serious these security threats are with China, and what you do in your office to make sure that that is something that we're encountering every single day that you can discuss. Obviously, this is sensitive information, but that's something that's clear in your policy documents.

Dr. PRABHAKAR. Yes, thank you for the question. The focus of this discussion, of course, has been on research security and the issues for the basic research enterprise. I think we've covered that ground pretty thoroughly. I think—

Ms. TENNEY. Well, I guess, let me focus it back to researchers, which is what we're talking about. These research proposals do go through rigorous scrutiny to make sure that that type of sensitive information is protected or disclosed to understand the China threat.

Dr. PRABHAKAR. Yes. I'd like to draw a distinction. When the PRC or its agents are going after conducting economic espionage, trying to get into classified networks, of course, we have very significant measures in place, an action is being taken. We—there have been many measures relating to export controls and financial flows for the basic research enterprise that we're discussing here. There—again, there—most of that information is widely available. It's intended to be public and globally shared. We understand that there are some sensitivities, for example, sensitive datasets, and in those instances, there are policies and practices that are in place or in development to make sure that we are protecting those aspects.

Ms. TENNEY. Thank you again for your work. I'm out of time. I yield back. Thank you so much, Mr. Chairman and Ranking Member.

Chairman LUCAS. The gentlelady's time has expired.

The Chair now turns to the gentlelady from North Carolina, Mrs. Foushee, for 5 minutes.

Mrs. FOUSHEE. Thank you, Mr. Chairman, and to Ranking Member Lofgren, for holding this hearing and to our witnesses today.

Dr. Prabhakar, I am honored to welcome you to the Committee today, and I look forward to you coming to my district in North Carolina next week to participate in our AI roundtable.

Artificial intelligence is a perfect example of the type of research we need to be thoughtful about when we talk about balancing openness with security. The United States must accept some level of openness will be necessary to catch up with China, which has advanced beyond us on certain AI technologies. However, AI is an example of dual-use research of concern, a technology that can be used for benefit or for harm. How does dual-use research of concern pose a unique challenge to OSTP as it develops policy guidance for Federal science agencies?

Dr. PRABHAKAR. Thank you so much for that question. I'm looking forward to being with not only you, but another Science Committee Member in North Carolina next week.

I think artificial intelligence is a terrific example of a powerful technology that—and we know how human beings—what human beings do with powerful technologies. They get used for good, and they get used for ill. And the research aspects of artificial intelligence, the basic foundation for this technology is something that we are—I think we are very privileged to have a number of American researchers and companies who have driven the major advances that have happened in the last year or so. But I think it's important to recognize that they, too, are part of a global community. Many of these companies have research going on around the world. Just as an example, the DeepMind company, now part of Google, is in the U.K., and they are one of the global participants in advancing this technology.

So I think we have great strengths, and it is rooted in global research. And then when we get to the applications of a technology like artificial intelligence, this is where we want to make sure that we here in the United States are using AI. Whether it's commercially or for public purposes, we want to make sure that we are moving really in a focused manner, moving fast, being aggressive about using this powerful technology in ways that are both responsible but also effective to achieve the great opportunities that it poses.

And something we've talked about a lot in this Administration is the fact that this—AI is a technology today that every country around the world is racing to use to build a future that expresses their own values. And coming back to the issues that we've been discussing with the PRC, I think we're all clear that we don't want to live in a future that's defined by technologies that have been shaped by authoritarian regimes, and so yet another reason that as we use this powerful technology that comes up out of a global base, that we make sure that we are racing ahead of everyone else to put it to work for all the things that we need to have happen.

Mrs. FOUSHEE. Thank you. How is OSTP considering AI specifically when it comes to the forthcoming policy guidance?

Dr. PRABHAKAR. I think of this research security program guidance that we are—that has to cover all areas of research, and in fact, that's one of the complexities because research is so varied. Artificial intelligence is an area of research in itself, and it is—increasingly, it is a component in every field of research. It's hard to find an area of research today that isn't using the power of AI with the data that it has to be able to accelerate what people are doing, so I think that it will be—the research security policies will affect many different aspects of AI.

Mrs. FOUSHEE. Would any other panelist care to comment?

Dr. RICHMOND. Yes, thank you. The Department of Energy has been working with AI, particularly in the secure side also, and so what we're working on is a FASST project, Frontiers of AI in Science, Security, and Technology. In this case, it's really important for this country to develop for science and technology in particular a big language model, a big model that pulls in a lot of data, that we can develop language models that help us go forward in AI in science and security. This is a kind of model that companies wouldn't be doing because they wouldn't have had the secure side, so I think for science and technology, there's something very unique that we need to develop in AI for this country to stay ahead in the area of science, technology, and security. And because that's a huge element of our laboratories, that's why our six big high-performance computers, our exascale computers are ideal for doing what the Nation needs.

Chairman LUCAS. The gentlelady's time has expired.

The Chair now recognizes the gentlelady from Oklahoma, Congresswoman Bice, for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman, and thank the witnesses for being with us this morning.

I want to start with Dr. Prabhakar, following up on an exchange that you had earlier with the Chairman on the research security

program requirements. Is OSTP committed to harmonizing the research security program requirements across all Federal agencies?

Dr. PRABHAKAR. Thank you for that question. That is exactly our goal, and I want to recognize again that Federal R&D spans so many different mission agencies, and there are different needs. In some instances, that's part of what we are wrangling in this inter-agency process that we're in, so we do want to make sure that we allow for sufficient flexibility. But at the end of the day, this won't work and be effective unless it's harmonized to a degree that allows our research institutions and universities to adopt and implement it sensibly.

Mrs. BICE. Great. Pivoting a little bit, I want to talk about foreign talent recruitment programs. It's been a big topic in this Committee in my time here. Dr. Keiser, if I may, Congress defined malign foreign talent recruitment programs in the *CHIPS and Science Act*, which OSTP pointed to in the guidance for Federal research agencies that was released yesterday. In your opinion, is the current definition sufficient to address concerns with malign foreign talent recruitment programs?

Dr. KEISER. Yes, and—so I have to say, we really appreciate the fact that there is a definition of malign foreign talent recruitment programs rather than a list because if we have a definition, it points to the very concerning aspects of these programs that are concerning to us from a research security and research integrity perspective.

Now, I do think that what we need to work on now is being very clear with this definition, so the definition has a part A, which is the concerning aspects, and then a part B, which is the countries of concern and those requirements. And then it also says international collaboration is excluded and is not part of this malign definition. So we have a big role now in communicating to the community of what this actually means. How can they identify what a malign program is, and how can they avoid being part of one?

And I'll give you an example. There's a U.S. researcher who signed an application to be part of a Chinese entity, to use his material science research for Chinese military purposes, and he's committing to do that. To me, clearly, that's a malign talent program. I don't know why he signed that, but certainly, we need to go out to institutions and make sure that this doesn't happen.

Mrs. BICE. Thank you. Do you think that Congress should address any of these concerns, maybe put more definitive sort of guidance out there? Or do you think it's—this is sufficient for now?

Dr. KEISER. So, you know, I think that, frankly, there is some room because there right now there's a part A and part B of the definition.

Mrs. BICE. OK.

Dr. KEISER. And my concern is that it might not be as clear as it could be.

Mrs. BICE. OK.

Dr. KEISER. And so I think that there is room, and we would be very happy to work with your Committee on some thoughts and making it even more clear.

Mrs. BICE. Perfect. Thank you for that. Pivoting back to Dr. Prabhakar, let me ask, do you believe that the Federal Government

is well-equipped to identify malign foreign talent recruitment programs? And what—if not, what resources do you believe are needed to be able to do so? And Ms. Richmond may also be able to sort of chime in on that as well.

Dr. PRABHAKAR. Thank you for that question because implementation here is key. The guidance that we've developed is an important first step, and very much to Dr. Keiser's point, now it's all about actually getting it out into the world. And I think we will learn more as we go along, but at the moment, I think the guidance is the first step that the agencies really need to be able to start being clear with all of the performers across the community.

Dr. RICHMOND. Yes, following up on that, and a good question, too, I think that that the guidance is a really good start, but as we learned from our experience in the—in our national laboratories, universities, this is a huge cultural change for them. This is a huge cultural change. And cultural change is going to be difficult because it goes all the way down to somebody working in a laboratory. And so it's going to be a real challenge for our universities to help through that cultural change. It's not just setting up an office. It's also us from our agencies because we fund universities, too, is to be able to work with them, to get them to trust us, that our process—

Mrs. BICE. Educating them.

Dr. RICHMOND. Yes, really educating them. And, you know—and to understand that—for all of us to understand that every time you go out of your house in the morning, you face risks, but you figure it's getting wherever you needed to go is the benefit. So we have to figure out where that balance is. And in our national laboratories and in the Department of Energy, we're used to seeing threats come in and not going oh, no, maybe we should just stop this person. Instead, we know how to do the balance of thinking about it more clearly, what other evidence, putting all the data together to come up with a decision. And I think the other agencies feel this way, too. But I think the universities need to be ready to let people know in their institutions, their researchers, that this is really important, and they need to think a little bit differently about how they've done things in the past.

Mrs. BICE. Thank you. My time has expired, Mr. Chairman. I yield back.

Chairman LUCAS. The gentlelady's time has expired.

The Chair now recognizes the gentleman from Florida, Mr. Frost, for 5 minutes.

Mr. FROST. Thank you, Mr. Chairman.

International collaboration among scientists, researchers, and thinkers accelerate the pace of progress such as—such cooperation strengthens and doesn't threaten our national security. For example, using NSF funds, the University of Central Florida (UCF), which is in my district, sends students to South Korea to study semiconductor chip production. The reshoring of chip production is a key national security and economic goal and a priority for our Committee.

Dr. Keiser, how do we make sure that American universities continue to have strong international partnerships and attract inter-

national talent while still securing their work from bad actors in unfriendly States?

Dr. KEISER. Mr. Frost, thank you very much for mentioning—this is a wonderful example that you mentioned about collaboration with South Korea and semiconductors. And this is what we have to do to our communities is we have to provide them with clear and tangible examples of beneficial, principled international collaboration and why it is. And we emphasize this in our research security training. We have a whole module on international collaboration.

But with the semiconductor example, you can clearly see the benefit to the United States. You clearly see the mutual benefit also to the other country, the partner. You see how they're both contributing to the enterprise and the partnership. And so to me, I think this is what we have to continue to communicate out.

The 2019 JASON report had a nice set of questions that one can ask to—and—to be sure and feel comfortable with the fact that you really are entering into one of these principled international collaborations. And the questions are very much along the lines of what I said. Also from our agencies we need to continue to communicate about the beneficial international collaboration and how it's just an essential part of science, but that we do have countries of concern that are not playing by these rules. And if that's the case, that's not collaboration.

Mr. FROST. Thank you. Dr. Lauer, disease doesn't respect borders. You know, improving Americans health has to be an international thing. At the University of Central Florida, we have folks who are researching HIV and patients in Panama, but the pace of this kind of health research can either mean lives lost or live saved. And so how do we make sure that research security efforts don't hinder, slow down lifesaving work like what we're seeing UCF do with HIV patients in Panama?

Dr. LAUER. Congressman, I completely agree with that sentiment. There have been a number of examples of strong international collaborations done right that have saved lives. One example would be NIH-funded work on Ebola and developing treatments and vaccines for Ebola that have turned this disease from being nearly uniformly fatal to being something that's potentially treatable and preventable.

I think one of the key points here is that we need to keep hammering in the message of both and not either/or. It's not either security and integrity or collaboration. The—it's both. It's both/and. And actually, we have used the criteria that Dr. Keiser referred to in that JASON report to help guide scientists and administrators into ways in which it's fairly straightforward to do things right.

Mr. FROST. Thank you. Do you have any other examples of collaboration between international researchers—

Dr. RICHMOND. I'm happy—

Mr. FROST [continuing]. That have led to important healthcare breakthroughs?

Dr. RICHMOND. Oh, you should continue.

Dr. LAUER. Yes. So I think HIV is another incredible example, and this is an example of where we have, over the years, converted HIV into a uniformly fatal disease. I remember that from when I was a medical resident in Boston. There was nothing we could do.

We saw these young patients die in front of our eyes. International work has now converted this from a uniformly rapidly fatal disease into a chronic condition. It's one of the amazing triumphs of modern medicine.

Mr. FROST. Did you want to add something, Madam Under Secretary?

Dr. RICHMOND. Not so much on the health side, but I have to point out that we have many international projects, for example, in high energy physics and nuclear physics and fusion physics and many other areas where these big facilities can't be built by just one country. They have to bring these countries together to do this. So on these huge projects, it's just critically important that we have these types of collaborations, so thank you.

Mr. FROST. Of course. Thank you so much, and I yield back.

Chairman LUCAS. The gentleman yields back.

The Chair now recognizes the gentleman from California, Mr. Obernolte, for 5 minutes.

Mr. OBERNOLTE. Well, thank you very much, Mr. Chairman.

Dr. Prabhakar, it's wonderful to see you again. I wanted to continue the line of questioning that Congresswoman Eshoo started about the competition with China with respect to artificial intelligence. And I know you and I have had several conversations on this topic. I remain very concerned about the fact that the United States is falling behind in that competition. I know you're aware that in 2017 the PRC made a national commitment to being the leaders in AI development throughout the world by the year 2030, and I think they're pretty well along. Most people are aware that several years ago they passed the United States in the number of computer science Ph.D.'s that they're awarding. They'll probably award more than double the number we award this year.

And you said something in your testimony that I thought was really interesting. You said it'd be very unwise for us to allow an authoritarian regime to shape future technology like AI. But I think it's particularly poignant here because, in addition to their investment in AI, the PRC has enacted some of the most stringent restrictions in the world on the commercial use of AI. So it's pretty clear they're seeing AI development through a military and a national security lens and not an economic lens.

You and I have discussed several times the Administration's Executive order that they issued several months ago on AI, and as I've shared with you before, I think that there was some really deep thinking in there about making sure that the United States remains competitive. What can we do, Congress and the executive branch working together, to ensure that the United States doesn't fall behind China in the race to develop advanced AI?

Dr. PRABHAKAR. It's great to see you again, Mr. Obernolte, and continue this important AI conversation. A very direct answer to your question is about the National AI Research Resource (NAIRR) and the AI Safety Institute. These are two components of making sure that we step up, first, to make sure that the data and the compute that are required for researchers broadly to get access to the ability to build and interrogate AI models, that's NAIRR, and then the AI Safety Institute is a new effort within NIST that's just getting launched. That is about making sure that we have the tools

and methods to be able to tell how effective and safe and trustworthy an AI model is. That is essential for everything that we need to do with AI. Those are two specifics that I would point to.

I really want to foot-stomp your comments. A number of years ago—when I was at DARPA a decade ago, I saw this huge surge in machine-learning technologies, this current generation of AI. I saw so many different applications for the work we were doing in national security and much more broadly. In the years—at that time, a lot of the concern we all had was that the PRC was using AI. Think about the amount of video surveillance information. Think about the amount of genetic information that that government has, those rich data sources used, again, expressing their values in building a surveillance state. They were—I think they surged ahead in the use of AI, and to my great delight, what has happened in the last couple of years is a surge ahead in the core technology with these large language models, again, largely—in that case, largely driven by American companies.

So we have this moment in time where we have phenomenal strength in this technology here in the United States. It is in the private sector. That's great. We want them to drive it, to accelerate it, to do it in a responsible way, but we also know that for public purposes and to make sure that we understand the safety issues with AI, that we need the public investment that exists across all of these agencies. You will find people using and building AI, but we know it's not adequate. And so this congressional support behind NAIRR and then the AI Safety Institute, I think, are two concrete places where we can make some critically needed progress.

Mr. OBERNOLTE. Right. Thank you. I think we're in furious agreement, especially on NAIRR, and I appreciate you highlighting that because we're trying to codify that and establish NAIRR permanently through the *CREATE AI Act*, which I'm—I and a few other people here are co-sponsors of. But thank you. We'll continue this discussion.

Dr. Richmond, in my remaining time here, I wanted to ask about research security at DOE, and you talked about how that's part of your core mission. But as co-Chair of the Fusion Energy Caucus, I couldn't help but think about multinational projects like ITER (International Thermonuclear Experimental Reactor) and the way that—you know, that's 35 different countries coordinating. How do you ensure research security when the DOE is just a small part of the international collaboration on that?

Dr. RICHMOND. Thank you for that question because it is something that we think about a lot with our large facility—with these large international facilities like ITER is an amazingly important project. There are scientific sides to it, and in any multi-country activity, there's going to be some political sides to it, too, and then some security sides to it. So again, we have—with the different security processes that we have in place, with our RTES and our risk matrix, we watch that very, very closely. It's—and it changes all the time, right? Every—all of this is evolving, but we've been there, and we just try to do the best that we can. But I'm very confident in the kind of people we have at DOE to make sure we're making the right decisions.

Mr. OBERNOLTE. All right. Thank you. I see I'm over time. I yield back, Mr. Chairman.

Chairman LUCAS. The gentleman's time has expired.

The Chair now recognizes the gentlelady from Pennsylvania, Ms. Lee, for 5 minutes.

Ms. LEE. Thank you, Chairman Lucas and Ranking Member Lofgren, for holding this hearing.

To probably go in a bit of a different direction as we continue to celebrate and uplift the contributions of countless Black inventors, scientists, and researchers during this Black History Month, I'm glad that today's hearing serves as a platform to further highlight the need for openness of opportunity as a tenet of scientific research.

It should be recognized that American research competitiveness has often failed to recognize contributions of the Black community and many others, and we must consider this when discussing strategies to maintain security over government-funded research and development. The memory of the late Eddie Bernice Johnson, the first and only Black person to ever chair this Committee, will continue to enshrine her legacy of providing access to career paths and opportunities in STEM for countless Americans, regardless of origin, across the country.

Prior to the 118th, only once has there ever been as much representation from Black women, for instance, on this Committee simultaneously. I'm proud to sit here today as part of another class of four with Reps. Foushee, McClellan, and Sykes. To reiterate, when I chose to be a Member of the Space, Science, and Technology Committee, I did so to help create a more equitable and just society, especially within the realm of STEM education and workforce. I continue to do so against the backdrop of unrealized dreams and potentials like those of Trayvon Martin who once aspired to become an astronaut. I also look forward to protecting proprietary technology and scientific discoveries such as that of Henrietta Lacks, that it never happens again.

I'm strongly of the position that the absence of Black indigenous people of color, BIPOC individuals in STEM research and development activities within Federal science agencies poses a significant threat to security and integrity of research outcomes. Without people like us not only hinders the scientific community from fully realizing its potential, but also jeopardizes the credibility and effectiveness of research efforts. So we can't tolerate racial profiling and racism as tools and ensuring research security.

While we must always be wary of threats our adversaries pose toward our Nation, my belief is that we are best served building resilience at home through supporting and developing the talent we have here at home. The people I represent look toward science and technology for innovation that will lower healthcare costs, bring clean air and water, and improve their living standards.

Dr. Keiser and Ms. Richmond, how are your agencies engaged in interagency collaboration with agencies like the Department of Education to promote science, history, education, especially the contributions of Black, indigenous, or people of color inventors, researchers, or scientists?

Dr. KEISER. Thank you very much for that question, Ms. Lee. And, as you can imagine, we are extremely concerned, and we believe that diversity in STEM is an essential part of research security. The security of our Nation is only able to occur if everyone is allowed to participate in the STEM enterprise. And so NSF did fund a \$10 million award to the University of Pittsburgh through the Eddie Bernice Johnson INCLUDES (Inclusion across the Nation of Communities of Learners of Underrepresented Discoverers in Engineering and Science) program, and this is to strengthen precollege STEM programs to ensure we're reaching the full geographic and demographic diversity of the Nation.

We, of course, also have many partnerships with other agencies, and everyone benefits from these investments. However, we need to do more. As you know, one of NSF's main priorities is the Missing Millions, and we need to make sure that we—all across NSF leadership, not just in one area, but across what we fund—focus on this very important enterprise effort.

Ms. LEE. Thank you.

Dr. RICHMOND. Well, thank you very much for that question. Both Rebecca and I have spent a lot of time worrying about this.

I do want to make one point, and it ties back to—on this particular issue. It ties back to the issue of the—you know, the number of graduate students, for example, that we have from other countries. Right now, our graduate stipends are so low in these emerging areas of technology that it's hard for graduate students to make a living during their 20's, 5, 6, 7 years in graduate school. Our graduate stipends across the agencies are too low, and it hurts our underrepresented groups more than others because, oftentimes, they don't come to graduate school with any parental finances to help them through or a car that can get them where they need to go. And so that is actually a huge factor in our inability to recruit and retain this talented group that we so much need. So the Department of Energy has stepped up and raised our graduate stipends to 45K a year, and I look forward to having the other agencies do that, too.

But I'm saying that we can't do this alone. I think it's really important that Congress step up and recognize that this is the kind of funding that we need to really get the young people into the system that are from all kinds of backgrounds because those are the ones that are left behind. And if we get those numbers up, we don't have so much need for those from countries of concern.

Ms. LEE. Thank you. Time moves fastest when we're having the most fun. I yield back.

Chairman LUCAS. Absolutely. The gentlelady's time has expired. The Chair recognizes the gentleman from New York, Mr. Williams, for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman.

Dr. Keiser, nice to see you again. You may not remember, but not quite a year ago, we first—this is where this topic first came onto my radar. And the concerns that you and a few others highlighted was that there were serious problems. There was movement to, you know, have rules change, but there was a gap in enforcement, the ability to enforce these rules. Can you update me at all from that conversation, either pro or con, of what's happened?

Dr. KEISER. So I think that what we've been doing as—in the past year is—No. 1 is we said making sure that we focus on consistency in approach. And what I mean by this is NSF works very closely with its Office of Inspector General. The Office of Inspector General does investigations into potential research security issues. They then make recommendations to NSF on actions, administrative actions it should take to reduce risk to the government. I believe that that's been a very close and good relationship.

What we've been working on in the past year is NSPM-33. As I mentioned, it says we should have information-sharing mechanisms because many of these researchers are funded by NSF, Department of Energy, and NIH, and so we all need to be able to share information when we do see concerns here.

So we've been doing two things. No. 1, we've been ramping up our own analytics efforts, and we've been sharing the information on what we see through those analytics with our partner agencies. We also make sure that our Offices of Inspector General also communicate very closely on these issues.

Mr. WILLIAMS. Thank you. Secretary Richmond, earlier, you commented about a Chinese researcher who was in fear of losing their grant funding and, I don't know, promised or pinky-promised or swore on a stack of Bibles that he was not related to the Chinese Communist Party. May I ask, have you ever been on a submarine, one of our nuclear submarines?

Dr. RICHMOND. No, I haven't had the opportunity yet.

Mr. WILLIAMS. Well, the crew ranges from about 110 sailors to about 160, and they are very fine people. And some of the secrets that are being stolen out of American research actually makes it easier for the Chinese Communist Party and the PLN, the People's Liberation Navy, to find our submarines—it's the most important deterrent weapon that we have—and their crews. And I'm just trying to weigh the difference between the sensitivity of the Chinese researcher who may lose his grants and the 110 or 160 sailors that are in our nuclear submarines off the coast of China today. I just wonder how you balance that.

Dr. RICHMOND. Well, thank you for that question. Let me go a little bit further with that to say what my advice was to this particular individual, having no idea of what his background was. I said the most important thing for you to do—because it wasn't so much losing his grant funding as it was that he would have to go back to China to do the kind of research that he wants to do here, which he would prefer not to be—not to have to do. But I said to him, the point is that we—research security is very important to all of our agencies. You will be—when you are putting in a proposal, you will be asked questions, and you need to be very honest and transparent with your university, as well as answering those questions about your current and pending support because that's what we will be looking at because we don't know whether to trust you or not.

So—but I said you're going to get in trouble if you don't disclose something and we find it. So that's why it's really important for whatever you're doing, that you be as upfront as possible with what your background is and give the responsibility to your univer-

sity, as well as your agency then, recognizing that you may be looked into it. But let me let me just also say——

Mr. WILLIAMS. If I may, just for the little bit of time that I have remaining——

Dr. RICHMOND. Yes.

Mr. WILLIAMS [continuing]. And I appreciate your concern for that person as an individual. I have a different perspective.

Dr. RICHMOND. Yes.

Mr. WILLIAMS. I'm pretty sure I'm the only Member of Congress that was in Tiananmen Square in May 1989 and visited Beijing University and the Freedom Wall, as you may recall. My very limited Chinese skills, at the time was very interested in what the protests were about. We didn't know what was coming at that point. This is after May 5 and before Gorbachev's visit.

But I would say that in my subsequent studies at Harvard University for a year as a visiting student in the Chinese Studies, Asian Studies Department, there were many of the Chinese leaders, student leaders that had been exiled at that time. And they were deeply concerned about, at that time, 1989, the direction of the Communist Party, and we now see it in full fruit. So I'm afraid that our kindness and our goodness are not a good defense against a really purposeful enemy. Thank you.

Dr. RICHMOND. I agree.

Chairman LUCAS. The gentleman's time has expired.

The Chair now recognizes the gentlelady from North Carolina, Ms. Ross, for 5 minutes.

Ms. ROSS. Thank you, Chairman Lucas and Ranking Member Lofgren, for holding this hearing, and I'm happy to see all of our witnesses here again.

As was mentioned earlier, we're very, very much looking forward to hosting Director Prabhakar in North Carolina next week, along with my colleague, Congresswoman Foushee, at our AI roundtable, which will be held at North Carolina Central University, an HBCU.

I represent a district that is home to the Research Triangle, boasting several top research universities, companies, startups, and Federal agency offices. And we've benefited greatly from international scientific research and the contributions from foreign-born scientists and international students. My first question, though, will go back to an issue that was touched on briefly, which is cybersecurity. And universities are increasingly the target of cyber attacks by both cyber criminals and nation-state actors to obtain sensitive information and prepublication research.

However, the cybersecurity of our research institutions has not been a central focus of research security discussions. To address this issue, the *CHIPS and Science Act* required NIST to produce cybersecurity guidance for universities conducting research. However, even with this good guidance, our universities often have tight budgets, and they're not fully able to address this guidance.

I see Dr. Keiser nodding first, so I will ask you how your agency is helping university awardees address cybersecurity risks as part of research security efforts. And then, of course, I want to go back to Dr. Prabhakar to describe your thinking about that.

Dr. KEISER. Sure, and I'll try to be brief. Something that we are going to be focusing on, No. 1, is NIH currently funds secure data enclaves. And we are tasked to also fund secure data enclaves at universities and through the—through our authorization. So we're in the process of developing that, No. 1, to provide that to the universities.

Second, the secure center that I mentioned is going to be partnering with the REN-ISAC (Research and Education Networks Information Sharing and Analysis Center), which is a cybersecurity consortium among universities to provide cybersecurity information and guidance out to them. So we're looking forward to that partnership as well.

And let me also just mention the importance, of course, of cybersecurity education. So we fund—as you know, at Duke in North Carolina and many other places, we fund CyberCorps and cybersecurity education programs. That's essential from the ground up to make sure that we have this as part of the culture.

Ms. ROSS. OK. Thank you.

Dr. PRABHAKAR. And I'll simply add that there's, of course, a cost to upgrading cybersecurity. That's true for any enterprise, including these universities. But of course, the reason we're doing this work is we know there's a cost to not doing it, and we just have to confront that.

Ms. ROSS. OK. Dr. Lauer, do you have anything to add?

Dr. LAUER. We're very grateful for congressional support on cybersecurity at NIH. It's become very much ingrained as part of our culture and also the culture of our extramural research systems, and so we very much appreciate that. We also work with institutions when unfortunate cybersecurity incidents occur.

Ms. ROSS. OK. Thank you very much. Back to the issue of international collaboration, many academic societies and Asian-American advocacy groups continue to raise the alarm about racial profiling in the research security space. According to a 2021 analysis from the Committee of 100, many of the highest-profile economic espionage cases tied to China have focused on academics, despite research institutions only comprising 3 percent of all cases investigated under the *Economic Espionage Act*. Given that this implies that bulk trade secret theft is not occurring at universities, what considerations are uniquely positioned within universities relative to industry? And, Dr. Keiser, I'd like to start with you.

Dr. KEISER. Thank you. The fear that the—those in the Asian-American research community have is real. It's real fear, and we need to acknowledge that, and we need to build trust and relationships. You know, I think—it breaks my heart when I hear stories about fear. I heard a story about, you know, some law enforcement agents during COVID, knocking on the door of a researcher of Chinese descent, and she wasn't quite sure why. This is something, of course, that we need to make sure that we deal with.

The way we need to do it in my view is, No. 1, build trust by interfacing. For instance, we have regular roundtables with the Asian-American Scholars Foundation (AASF), and that's something that we need to do to not only communicate to them, but to listen to them and think about ways we need to collaborate together in this area.

The second thing we need to do is make sure that our actions are scaled to the risk. So we—that’s why I mentioned the information-sharing on research security violations. We need to focus on the behaviors and the fact that we are not looking at the people and their backgrounds. That’s hard, I think, for many to accept because we don’t have the trust yet, so we need to give out more examples of the fact that this is what we’re doing, as well as something in my view that I’ve talked to the AASF about is we have to give examples of when someone came forward and corrected an error, and we didn’t take action because it was corrected. Those kinds of things have to get out there as well.

Ms. ROSS. Thank you. My time has expired, and I yield back.

Chairman LUCAS. The gentlelady’s time has expired.

The Chair now recognizes the gentleman from Florida, Mr. Franklin, for 5 minutes.

Mr. FRANKLIN. Thank you, Mr. Chairman. And this is such a critical hearing today, and obviously, we feel that tension between the trust that we need to build in the scientific community, but also protecting our national security.

Dr. Lauer, last year, you published a summary of NIH’s foreign interference cases. And to date, NIH has determined that 80 percent of compliance reviews had at least one serious violation, and in total, over half of the scientists were removed from NIH grants. Now, those stats are obviously very concerning. What actions can be taken to further prevent violations? As important as compliance reviews are, it’s kind of a bit of the horse is out of the barn at that point. What can we—are there things we can be doing to get out ahead of that and lower these stats by having those violations not be there to begin with?

Dr. LAUER. That’s a really great point. And I think one of the possible signs of success to date is that the number of new allegations that we have seen has declined substantially since 2019, and most of the new allegations that we have seen have actually come from institutions themselves where institutions on their own discovered that there were problems as part of their outreach and due diligence. And so that gets exactly to your point, that what we really want to do is promote a culture of both openness, as well as integrity and security.

Mr. FRANKLIN. OK. Do you have the resources you need for—to perform these audits and do the measures like that?

Dr. LAUER. Over the last few years, we have received additional funding. Our office has received additional funding from Congress to help us with our compliance reviews, also with our IT and our analytics. We are very grateful for that support, and we hope it will continue.

Mr. FRANKLIN. OK. According to NIH Central Resource for Grants and Funding, approximately 80 percent of NIH’s budget goes to support research grants, including grants to foreign organizations. And in the spirit of being collaborative, many of your grant dollars come without restrictions on them, which is—again, goes to building that spirit of trust and collaboration. How can we be sure these investments, especially those made with foreign countries, are protected from our adversaries?

Dr. LAUER. So any grant that involves substantial work in a foreign entity has what we call foreign components. And before we allow those foreign components to go forward, we require what we call a prior approval. That involves consultation with the State Department. We give the State Department then an opportunity to comment on whether or not there may be any foreign policy concerns regarding that project. So we have built-in steps in place in collaboration with the State Department to try to head that off.

Mr. FRANKLIN. OK. And then I've got a couple of minutes left here. I'd love to follow up a little bit more, Dr. Richmond, and then also get your thoughts, Dr. Prabhakar, on the—you know, one of the aspects of research security that we don't focus on a whole lot is retention of the workforce. And, you know, we—obviously, if folks don't feel trusted or they feel threatened, they may leave and go elsewhere. But I'd love both of your thoughts on how can we work harder to build that trust that we need to, you know—what can Congress do to assist you in helping to develop an ecosystem that facilitates that trust that we need to ensure that the folks that we have that come to our institutions, that get educated, they got great things to offer aren't just simply hired away by the CCP? And it's one thing to be inside the program and stealing, but another if we can't retain them when they go elsewhere. It's the same effect. We have the brain drain.

Dr. RICHMOND. Yes, that's really a tough one because changing culture isn't easy, and changing culture means that people trust what you've got at your institution.

I think that, you know, I can reflect on the fact that the National Laboratories operate in many respects further ahead than our academic institutions because when you come into work in one of our laboratories, there is a culture that—we have a safety culture that's really, really important that's embedded in—woven through everything. And there's also security aspects that's woven through everything that we do.

So you think about safety and security all—and, I mean, just, you know, falling off a ladder. But the point is that we've developed that culture in the laboratory so that somebody that's coming in, like you would hope they would come into a university, wanting to get grant money, that they buy into that culture when they first come in. And it's trusted because it's been there for a while.

And so I think being able to get universities to the point where security is woven into everything that they are doing so the researchers really understand that this is about the Nation's competitiveness in particular areas. In this case, there are six particular areas that we worry about with regards to AI and quantum and bio and—six different areas. But it's those areas that we've built that culture around, so that's what I would say.

Mr. FRANKLIN. Well, I appreciate your comments. And, Dr. Prabhakar, sorry, I'm out of time, but I would love to get your feedback maybe later on, you know, how do we develop that ecosystem so that we retain the best and brightest and while we still have that trust that's necessary?

Dr. PRABHAKAR. Thank you.

Mr. FRANKLIN. But thank you, Mr. Chairman. I yield back.

Dr. PRABHAKAR. I appreciate it.

Chairman LUCAS. The gentleman's time is now expired.

The Chair recognizes the gentleman from New York, Mr. Tonko, for 5 minutes.

Mr. TONKO. Well, thank you, Mr. Chair. I thank the Chair and Ranking Member for holding this hearing, and thank you to our witnesses for being here today, and more importantly, for your excellent leadership in supporting our Nation's research enterprise.

As many of you noted in your testimonies, research integrity is a key part of research security, and research integrity is buttressed by strong and uniform scientific integrity policies. With the influx of new resources from the landmark *CHIPS and Science Act*, it is important to ensure that we can make the most of this opportunity to strengthen the U.S. research enterprise and keep it clear of all threats to research security, including domestic political interference, distortion, or indeed disruption.

Scientific integrity is a cornerstone of Federal scientific activities and something that I've made a priority during my time in Congress by authorizing the *Scientific Integrity Act*. So a question to the entire panel, how could stronger and more uniform scientific integrity policies help mitigate risks in research security and integrity? Anyone want to start? Mr. Lauer?

Dr. LAUER. Thank you. So I think integrity and security very much overlap, and virtually all the cases that we have seen there have been integrity breaches, the integrity breaches often manifest themselves as dishonesty, outright misrepresentations of certain past activities.

So I am reminded of a report that was put out by the National Science and Technology Council in 1999 about the government-university partnership, and it pointed out that one of the core principles, exactly as you say, of a successful research enterprise is integrity, and specifically the integrity of every individual participant. When there is a breach of integrity, that threatens the credibility of the entire enterprise, and that means security as well. Thank you.

Mr. TONKO. Thank you. Anyone else on the panel?

Dr. RICHMOND. I think to say that the—you know, we are as secure as our weakest link, and so that's why it's important for us to focus on a broader spectrum of issues that we're looking at than we might have in the past. I also think what would be helpful is, with the *CHIPS and Science Act*, that part of that is just authorized and not appropriated yet, and I think that would help us go forward, too.

Mr. TONKO. Sure. Thank you.

Dr. KEISER. And I'll just add that research integrity, of course, is essential to what we're talking about. What we also are starting to focus more broadly on is overall foreign malign influence because, as you said, there is the integrity of the research itself, and then there is the way that other countries are causing fear or manipulating faculty members, et cetera, that are violating freedom of speech, that are violating academic freedom, that are intimidating them. So to me, we have to look at the broad picture, including integrity and including these other areas of foreign malign influence.

Mr. TONKO. Thank you. Dr. Prabhakar, since research integrity and scientific integrity might be discussed as two sides of the same

coin, how would you recommend the agency structure policies related to that research security and scientific integrity to leverage these commonalities?

Dr. PRABHAKAR. Thank you so much. I think my colleagues actually spoke to this so beautifully. And I think it's worth recognizing that the purpose of the scientific enterprise is always to improve the scientific process and to get better and better at understanding ground truth. And that, to me, is what scientific integrity is all about. And I think Dr. Keiser made an important point about that, that is complementary to protecting against illicit activities from countries of concern. But they all get wrapped up in a package of what are the behaviors. And to the Under Secretary's point, these are cultural issues about how we conduct the science and technology that's so important for our country.

Mr. TONKO. Thank you. Well, scientific integrity is a key ingredient in securing our research enterprise, and I hope that this Committee and the Administration can continue to work together to ensure strong policies across our Federal research landscape.

Another piece of research integrity—and therefore, research security—is ensuring our researchers and institutions conduct rigorous, reliable, and replicable research. Dr. Keiser, in your written testimony you discuss the importance of safeguarding taxpayer investments to research security. How can agencies help safeguard taxpayer investments and ensure that Federal funding is being used for that replicable and reliable research?

Dr. KEISER. So I think over—what we have been doing quite a bit—and, frankly, there's a lot more to do. We have instituted additional training for our program officers and program directors because what we want to do is make sure that the researchers themselves whom we fund have the freedom to conduct their research, but we also have to be very clear and communicate to our program officers that their job is to ensure that the—of the reliability and the integrity of the research itself and the research projects.

Now, I have to say that this is a challenge because one program officer can be overseeing 100 projects at one time, but I think that it's extremely important to make sure that there is that oversight, to make sure that the funds are used as the researcher says they're going to be used, that they produce results that are then made open and that are reliable.

Mr. TONKO. Thank you very much. With that, my time is exhausted, and I yield back.

Chairman LUCAS. The gentleman's time has expired.

The Chair recognizes the gentleman from Alabama, Mr. Strong, for 5 minutes.

Mr. STRONG. Thank you, Chairman Lucas and Ranking Member and our witnesses for sharing their expertise today.

Dr. Keiser, I'm sure we can all agree that we need ways to cultivate and grow our workforce that understands research security and that we can work in an academic setting. I often hear from researchers in my district that they are hesitant to work on restricted research due to the constant hurdles they must jump through. What are some of the nuisances involved in training a workforce prepared to deal with the growing research concerns in academia?

Dr. KEISER. So NSF, when we fund research, we fund fundamental research, and we ensure that it is not restricted research. That being said, that's why education is so important because that doesn't mean that everything should just willy nilly occur in a lab without the safeguards that we talked about being put into place. That's why we have to provide the resources for research security programs, to make sure that they understand, as Dr. Richmond said, that what we want to create is a culture like a lab safety culture but of research security without these additional restrictions.

Now, the JASON reports have spoken out quite strongly that they do not like controlled but unclassified information, and that is something, of course, by law that we do need to deal with. And so I think that's something that our agencies are trying to figure out how to fund CUI (Controlled Unclassified Information) research in a way that doesn't provide—that doesn't cause additional administrative burden on labs, et cetera, and that's by building a culture.

Mr. STRONG. Thank you. Are there ways to involve law enforcement and intelligence and the intelligence community in this workforce development?

Dr. KEISER. Yes. And I have to say we work very closely with the intelligence community and law enforcement. If you look at where we started in our communication as far as what research occurs and how research occurs in the academic setting, when we started this conversation in 2017, it was two completely different lenses through which we were looking. We now communicate very closely. NSF and DOE and HHS (Health and Human Services), we're part of the National Counterintelligence Task Force where we have these conversations and we need to work together.

And so I think that we've come much more to a good understanding of how research occurs in the labs. At the same time, we need to still move forward, frankly, with the researchers themselves understanding what it really means to safeguard this research, so more work to be done.

Mr. STRONG. Thank you. How can NSF promote a strong research security workforce at our universities? And how can Federal agencies better leverage expertise in cities like Huntsville, Alabama, which is home to the second-largest science and technology research park, to train the future workforce?

Dr. KEISER. Yes, it's—I'm so glad you mentioned training the next generation of research security workforce. I've been thinking a lot about this because I do feel if we're going to promote this culture, we need to figure out a way to encourage and support the workforce in research security, that understands this balance between openness and research security. So what I'm thinking about is we're establishing a Research on Research Security Program, a funding program, and I would like to use an element of that funding program to train that generation—next generation of research security workforce.

Mr. STRONG. I think one of the great statistics that I've learned in recent days, the University of Alabama in Huntsville, 72 percent of their graduates never leave. They stay in the research park, in Redstone Arsenal area, and I think that that right there shows a lot of hope for what all of us are concerned about.

Dr. KEISER. Absolutely, creating that culture.

Mr. STRONG. Thank you. Dr. Lauer, many international students take advantage of optical—Optional Practical Training, OPT programs, which allow them to obtain employment in the United States for up to 3 years post-graduation. In 2022 OPT benefited more than 117,000 students with F-1 visas. How can we assist research institutions in coordination of DHS (Department of Homeland Security) to screen foreign national students and restrict potential bad actors from receiving OPT authorizations?

Dr. LAUER. So this is not an issue that I have or our office has been personally dealing with, so I think what would be best would be for me to research that and get back to you.

Mr. STRONG. Thank you. According to the NIH Central Resource for Grants and Funding, approximately 80 percent of the NIH's budget goes to support research grants, including grants for foreign organizations. In the spirit of being collaborative, most of your grant dollars come without restrictions. How can we be sure that these investments, especially those made in foreign countries, are protected from our adversaries?

Dr. LAUER. So as part of our standard processes, whenever a grant involves substantive work that's occurring in a foreign country, we require what we call prior approval, and that—and this is prior approval for what we call a foreign component. And what we do is we work through the State Department. Every such grant like this is then sent over to the State Department for their review, and they will then inform us if there are significant foreign policy concerns.

Mr. STRONG. Thank you. Mr. Chairman, I yield back.

Chairman LUCAS. The gentleman yields back.

The Chair now recognizes the gentleman from Indiana, Dr. Baird, for 5 minutes.

Mr. BAIRD. Thank you, Mr. Chairman. And I thank the witnesses for being here. I always learn something in these meetings with the talented witnesses that you have here.

But, you know, I got to tell you, Mr. Chairman, I really appreciate serving on a Committee with you. You're very organized, you're very methodical, and I know exactly what you expect of me, so I commend you on that.

Chairman LUCAS. You are a great underclassmen.

Mr. BAIRD. But, you know, I have a research background, and so the issue we're talking about here today, I strongly believe that research is going to be our way to stay ahead of the rest of the countries in this world, including some of our adversaries, and so I really understand the open platform and the reason for that. If you have an open platform, you don't have to reinvent the wheel every time. But as every one of you have mentioned, the concern is how do you do that, keep people stimulated. And I've heard you say that, but I still want to emphasize that we do have to pay attention to what our adversaries are doing. And sometimes it seems innocent, but the piece of information they get may be key. And I know you know that, but I just want to reemphasize how important I think that is.

So my first question is, Dr. Lauer, this Committee has heard from researchers that they're blamed when identifying foreign threats, as it reveals a weakness in their security systems. So how

can the Federal agencies sincerely protect and support our researchers to address vulnerabilities without impacting their strength to identify threats?

Dr. LAUER. So I think a major part of this is enhancing a culture in which it is understood that we can have both integrity and security, as well as strong science and strong international collaborations. And in many respects, we get quite practical. Dr. Keiser referred to the JASON report, which has some amazingly good advice, which we've actually used, to help individual scientists, as well as university administrators develop international collaborations that do exactly what you're saying, that assure high-quality science, effective science, but at the same time, ensure that the interests of all parties are being appropriately protected.

Mr. BAIRD. Thank you. Dr. Prabhakar, the *CHIPS and Science Act* that we passed here a year or so ago directed the development of the training modules for NSF that was launched last month. The legislation also requires a certification that all federally funded grantees complete an annual training on research security policies and foreign threats. So how do you expect universities to certify this requirement before the research security program guidance is finalized?

Dr. PRABHAKAR. Thank you for that question. And that, again, is part of the urgency. I'm failing to get that done and to wrestle through all the complex issues that we're struggling with on the research security programs. The *CHIPS and Science Act* was—is such an important step forward, the training piece is critical, and I know that NSF has been able to make some good progress with that.

The *CHIPS* R&D component at the Department of Commerce is ramping up now that—we had a great launch event last week for that, and I know that Secretary Raimondo is particularly focused on that—on the workforce components. So, again, I think that's—getting that right is—I completely share your focus on that.

Mr. BAIRD. So do either of the two of you left have any comments in that regard?

Dr. KEISER. We look forward to coordinated, of course, on the research security program standards, and we also are moving forward with a certification of the training. So we're entering it into our policy guide that the researchers on NSF grants who usually also get grants, I said, from these other agencies are going to need to certify that they've taken this research security training.

Dr. RICHMOND. Yes, and I would say that at the Department of Energy, we're coordinating very much with our other agencies to make sure that the training that we provide is consistent with what everyone else is doing. It is a—it's an evolving issue, and we have to make sure that the training that we create evolves with the threats that come to us, so thank you for that.

Mr. BAIRD. Thank you. And you completed well on time. Mr. Chairman, I got 9 seconds left, so I yield back.

Chairman LUCAS. I am impressed, Doctor. I'll let an Indiana Member question any day.

With that, we turn to the gentleman from Georgia, Mr. McCormick, for 5 minutes.

Mr. MCCORMICK. Thank you, Mr. Chairman, appreciate this and this topic especially.

We recognize the United States as the leader in research and development with some of the brightest minds and the greatest ideas. We don't always support the R&D the way that people want to, sometimes from government, sometimes from private entity, but collaboratively, we've been leading the way in AI production for—since the beginning of its inception.

Research and innovation are the crux of the American dream. The idea that people from all over the world with different backgrounds can achieve success and prosperity through hard work, determination, and initiative is the basis of our society. Just a few weeks ago, I had the pleasure of visiting the AI hub at Georgia Tech. We had three silos. It's amazing. I watched this production of amazing technology where you get to actually design the hardware and software together to work in this next advancement in technology so we can do some really special things. In Georgia, I think, when we lead the way—three of the silos of the 30 are right there in Georgia, which I'm really excited about and how it can apply to everything from healthcare to engineering to literature, and you name it, that is the future.

With that being said, though, we live in a time where real national security threats exist, and we must ensure that our universities and research systems have clear guidance to place—in place to ensure that we are safeguarding our critical research programs from foreign adversaries, specifically, the Chinese Communist Party. I've watched them develop their AI over time. They've invested a tremendous amount of resources all from their government, all guided by them and a lot of times for nefarious reasons. And they also were produced with their slave labor and their manipulation in the market, a very cheap product.

Unfortunately, all of our AI production is in Taiwan, which the Chinese Communist Party has openly said they will take by 2027. And the *CHIPS Act*, by the way, didn't solve that, so I'm very concerned.

Dr. Lauer, recent reviews of the Health and Human Services Office of Inspector General and GAO have raised questions about the NIH and its effectiveness in monitoring and overseeing its ward recipients, particularly for grants involving foreign subrecipients. In January 2022, HHS Office of Inspector General recommended that NIH implement enhanced monitoring documentation and reporting requirements, quote, “for grants with foreign subrecipients,” and NIH agreed with the recommendation, but subsequently stated that it may need to obtain additional authority.

My question is this. Can you elaborate on what additional authorities are required and what steps the NIH has taken to implement this recommendation?

Dr. LAUER. So I think we have some good news there, which is that we've been able to implement all the recommendations from that audit. One of the things that we did was that we provided a guidance or a clarification guidance that indicated that all foreign recipients have to make available to their prime domestic recipients information that informs progress reports, so that would include laboratory notebooks, original electronic files. And they have

to do this in a timely way, which would typically mean at least once a year, if not more often than that.

We put that out in the *Federal Register* last June. We received comments, we responded to the comments, and we put out a final policy last fall. And that policy is now in the process of being implemented.

Mr. MCCORMICK. OK. I just want to point out that whether it be the World Trade Organization, the World Health Organization (WHO), which China belongs to both and has manipulated brilliantly in the over 20 law cases which they lose, and then it gets better cheating. The WHO was we have serious questions about what happened with COVID and its development. Just another agreement with other foreign subsidiaries and recipients doesn't really go into accountability. Just because we have an agreement doesn't mean you don't cheat, and it goes into arms wars and everything else that we've seen the international community cheat at. So I don't want to just see rules and agreements. I want to see oversight and accountability, which is the bigger part and the harder part of what we do. And could you address that?

Dr. LAUER. We completely agree. And, as you may know, we've had a case in which a foreign subrecipient refused to provide information that our agency was requesting that resulted in termination of their subaward, and even more than that, it led to debarment of that foreign institution for 10 years. So we do take accountability very seriously, completely agree with you.

Mr. MCCORMICK. OK. I want to point out, too, that even in drug production, amoxicillin, Augmentin, and other drugs that we have produced overseas specifically in the CCP, that we do a very poor job of holding them to the same standard we have our own people held to account. In other words, we investigate our hospitals, our drugmakers, our manufacturing constantly, and yet the very things we rely on China for safety and production, we don't do, and when we do it, we give them announcement, we give them warning, and we do it very infrequently. So accountability is something we need to do a much better job of those foreign subrecipients than we do with our own people.

And with that, I yield.

Chairman LUCAS. The gentleman yields back. The gentleman's time has expired.

It appears that all of our colleagues who were available for questions have asked their questions. Therefore, I want to thank the witnesses for their valuable testimony, and of course, the Members for their questions. This has been a very productive hearing.

The record will remain open for 10 days for additional comments and written questions from Members. The hearing is adjourned.

[Whereupon, at 12:30 p.m., the Committee was adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

*Responses by the Honorable Arati Prabhakar***Responses to Questions for the Record for Arati Prabhakar**

Director of the White House Office of Science and Technology Policy and
 Assistant to the President for Science and Technology
 before the House Committee on Science, Space, and Technology
 Hearing on “Examining Federal Science Agency Actions to Secure the U.S. Science and
 Technology Enterprise”
 February 15, 2024

Chairman Frank Lucas**1. What is the role of the Committee on STEM Education in coordinating research security policies across the federal government?**

Matters of coordinating research security policies across the federal government are carried out by the National Science and Technology Council (NSTC)’s Subcommittee on Research Security.

2. Given the congressional directive to develop a national S&T strategy, how is OSTP planning to engage with international partners and stakeholders to develop strategies and best practices for safeguarding sensitive research on a global scale while preserving the open and transparent nature of the global research enterprise?

OSTP, the National Security Council, the State Department, and other government agencies actively engage international partners and stakeholders, including the Five Eyes countries and G7 members, as well as other partners, on developing strategies and best practices for safeguarding research while preserving the open and transparent nature of the global research enterprise.

3. This Committee’s first hearing of the 118th Congress focused on considerations for developing a National Science and Technology Strategy that ensures a comprehensive, whole-of-government approach to research and development and maximizes the return on taxpayer-funded investments. Congress directed OSTP to develop this strategy no later than one year after the completion of the quadrennial science and technology review. This Committee expected the quadrennial review to be completed by December 31, 2023. Please provide a detailed update on OSTP’s progress toward completion of the quadrennial review? When do you anticipate its completion? Which subcommittee or working group is responsible for completing the quadrennial review?

The CHIPS and Science Act of 2022 requires OSTP to conduct a quadrennial science and technology review (QSTR) of the federal science and technology enterprise. As part of a comprehensive examination, departments and agencies with significant R&D investments provided an overview of their efforts on the topical areas identified in the CHIPS and Science Act to OSTP. The QSTR will be submitted to Congress and released publicly by OSTP upon completion of applicable review processes.

- 4. What subcommittee or group will be responsible for developing the National Science and Technology Strategy following the completion of the quadrennial review? When do you expect to deliver that strategy to Congress?**

The CHIPS and Science Act of 2022 requires OSTP to develop the National Science and Technology Strategy following the completion of the QSTR. OSTP's Industrial Innovation team is coordinating this work, and we anticipate completing the requirement by the deadline.

- 5. The Committee on STEM Education was scheduled to release an update to the 5-year federal STEM education strategic plan in December 2023. What has caused the delay in the release of the updated strategy?**

In 2023, the Committee on STEM Education implemented the fifth year of the 2018 federal STEM education strategic plan. Last year, the Committee on STEM Education was also re-chartered and re-named the Committee on STEM (CoSTEM). Over the course of 2023, interagency working groups (IWGs) were sunset and, to support new CHIPS and Science Act provisions, new IWGs were formed. Much of 2023 was spent expanding membership in CoSTEM to incorporate new agencies, advancing CHIPS and Science Act provisions, and carrying out significant external and internal engagement as inputs to the new strategic plan. CoSTEM expects to release the new five-year strategic plan for developing STEM talent this year.

- 6. On February 12, 2024, OSTP updated the list of Critical Emerging Technologies. What was the motivation behind expanding the list to include subfields for each CET?**

The Critical and Emerging Technologies (CET) list has contained subfields since its 2022 update. The 2024 list's subfields help provide specificity for the CET list's diverse audiences, particularly in broad technology areas like "Space Technologies and Systems" or "Clean Energy Generation and Storage."

- 7. On January 14, 2021, President Trump issued National Security Presidential Memorandum 33 (NSPM-33), "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," which tasked OSTP and the Subcommittee on Research Security with coordinating the implementation of these provisions across federal agencies to secure federally funded R&D. How do you intend to monitor consistent application of NSPM-33 across agencies, and ensure that U.S. researchers are familiar with NSPM-33 and agency expectations, especially where normal scholarship and international collaborations and conferences are involved that may diverge from NSPM-33 guidance? Will guidance be both proactive for the future as well as retroactive for previous international collaboration and activities?**

To ensure consistency, OSTP has required that research agencies submit to OSTP their plans for implementation of the harmonized common disclosure forms for the Biographical Sketch and the Current and Pending (Other) Support portions of funding application packages for grants and cooperative agreements. These will also be reviewed by the Office of Management and Budget, which will be responsible for reviewing deviations from the common forms. OSTP intends to utilize similar measures for other elements of NSPM-33, such as research security programs.

OSTP guidance is intended to be proactive for future international collaboration activities, as retroactive application could require large-scale renegotiation of extramural award terms for past awards.

Rep. Darrell Issa

- 1. For decades, the United States has pursued broad-based research science and technology collaboration with the People's Republic of China, especially between academic institutions in the United States and China's universities.**

- a. To what extent does the United States rely upon the PRC's research and development apparatus for our scientific advancement?**

The U.S. continues to lead the world in R&D. As the PRC increases its research investments, it increasingly has experimental capabilities that do not exist in the U.S.

- b. Do your agencies assess if this broad-based cooperation continues to be in the United States interest? If so, why?**

The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it. This means that we must be selective in the areas in which the U.S. government collaborates with PRC entities and that we continue to demand adherence to norms of transparency and reciprocity that underpin the global research enterprise.

As the PRC produces more knowledge through its growing investments in science and technology, it will increasingly be the case that gaining access to some of that knowledge through collaborative efforts would be in the U.S. national interest.

Similarly, the PRC's efforts to increase its interests in multilateral technical fora require constant U.S. attention and engagement to ensure that we can strengthen and maintain the normative frameworks that underpin the global research enterprise. Consistent with the National Security Strategy, this allows us to align our efforts with our network of allies and partners, acting with common purpose and in common cause, and compete responsibly with the PRC to defend our interests and build our vision for the future.

- c. Are benefits derived from such broad-based cooperation reciprocal to both the United States and the PRC?**

In an increasing number of areas, PRC counterespionage and data laws and the vagueness of how they are implemented have made it difficult to engage in transparent and reciprocal cooperation with U.S. and global research institutions. However, as noted above, the absence of the U.S. from collaborative efforts increases the likelihood that there may be key breakthroughs without U.S. involvement.

- d. PRC nationals make up a sizable number of graduate students in U.S. STEM fields.**

- i. Is the U.S. domestic research enterprise dependent on individuals from the PRC?**

According to the National Science Board report “Talent is the Treasure” released in March 2024, a substantial and growing proportion of the U.S. science and engineering workforce is foreign born, led by talent from China. This is particularly true among computer and mathematical scientists as well as engineers, where more than 50 percent of all doctorate holders are foreign-born.

ii. Could this talent pool be replaced by nationals from partner countries?

While the 2023 Open Doors Report on international students produced by the Institute for International Education and multiple State Department reports, find that the decreasing number of student visas from the PRC has been offset by individuals from other nations, we have not seen a corresponding offset in the number of non-student international scholars from countries other than the PRC as the number of Chinese scholars has declined, even as other scholars returned after COVID-19 restrictions eased. Overall, the number of individuals on international scholar visas in the U.S. has declined by about 25 percent since 2018. The report notes that 79 percent of international scholars focused their academic activities in STEM fields.

As noted in the recent report “Characterizing the Loss of Talent from the U.S. STEM Ecosystem” by the Science and Technology Policy Institute, the decline in the number of international scholars in the U.S. is likely partially attributable to the increasing global competition for international talent, including efforts from our allies and partners to make it easier to attract and retain talent. The report notes, though, that the U.S. remains a highly attractive destination for highly skilled workers and that roughly between 55,000 and 75,000 temporary foreign workers join the U.S. STEM workforce each year based on H1B visa statistics. State Department data shows over 200,000 H1B visas were issued annual in fiscal years 2022 and 2023, which exceeded the pre-pandemic levels. Employment-based immigrant and non-immigrant visas are critical to the U.S. talent pipeline and fueling the U.S. research ecosystem. Overall, more than 40 percent of doctorate holders in the U.S. science and engineering workforce are foreign-born.

e. Given General Secretary Xi Jinping’s expansive understanding of “national security” do your agencies assess that research collaboration with the PRC on STEM technologies is inherently dual-use? If not, why not?

Basic research is defined as research directed toward increasing knowledge and understanding in science and engineering, rather than the practical application of that knowledge and understanding. Because of this, it is difficult to characterize all research collaboration as inherently dual use, regardless of the PRC’s expansive understanding of national security.

2. Fundamental research has long been exempt from export controls. Despite significant advances in our understanding of the Chinese Communist Party’s technological ambitions and strategy, this policy has yet to be revisited.

a. Do you believe the time has come to reevaluate National Security Decision Directive 189?

There are no plans to reevaluate National Security Decision Directive 189, particularly given that federally-funded basic and applied research under NSDD-189 may still be subject to classification controls if the unintentional disclosure of information could cause harm to national security. The fields of development present the greatest risk are largely funded and performed in and by the private sector and are outside the scope of NSDD-189. This is also the position articulated in the 2024 JASON report on research security.

b. Do your agencies assess that fundamental research is necessary for the PRC to achieve the goals of its Made in China 2025 industrial policy?

It is highly unlikely that fundamental research conducted today would be successfully translated into development in the timeframe of the Made in China 2025 industrial policy. All countries rely on fundamental research as an important first step in the discovery process, and the PRC is investing heavily in capabilities and capacity building that will allow it to become a world leader in fundamental research that may eventually be translated into industrial development activities.

c. Do your agencies assess that basic research collaboration and knowledge transfer of fundamental research support People's Liberation Army modernization?

Given that basic research is defined as “systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind,” it is often difficult to draw a line from basic research to technological outcomes. However, given that basic research is an important first step in the innovation process, most technological outcomes are also derived from earlier basic research activities.

d. Can you describe the benefits that would result from stemming the flow of basic research to the PRC?

The 2024 JASON Report on Safeguarding the Research Enterprise notes that controls on research would impose significant cost on the conduct of research, reduce research funding efficiency, shrink the talent pipeline, and “create hinderances for education, the progress of science, and national security.” A similar study conducted by the Defense Science Board in 2023 came to a similar conclusion.

Stemming the flow of basic research to the PRC would inherently require limiting access for U.S. researchers, thereby severely limiting its impact, undermining the scientific community's ability to validate scientific findings, and cutting off potential avenues for the U.S. to translate our own research into innovation. Such restrictions could also encourage the PRC, in addition to even U.S. allies and partners like the European Union, to take similar measures in response, thereby further stemming the flow of new knowledge to the U.S..

As noted earlier, government-funded basic research, which could be used to harm U.S. national security, may still be subject to classification.

- 3. Since the China Initiative's termination, have any of your agencies experienced a shift in the willingness or ability of the Justice Department to pursue criminal cases related to research security violations and intellectual property theft from China?**

No, OSTP has not.

- 4. On November 8, 2023, I led a group of Members in sending a letter to Secretary Blinken, Secretary Raimondo, and Ambassador Tai requesting that they pause negotiations on the U.S. China Science and Technology Cooperation Agreement (STA).**

- a. To your knowledge, what is the status of STA renewal negotiations?**

Negotiations to amend and strengthen the terms of the U.S.-PRC STA are on-going.

- b. Do your agencies assess that the United States derives reciprocal or substantial benefits from maintaining a broad-based research cooperation agreement with the PRC rather than specific agreements on discrete topics, such as influenza?**

Yes. The STA is a framework that provides consistent standards for government-to-government scientific cooperation, and it does not obligate the U.S. to engage in S&T cooperation with the PRC. Specific agreements on discrete topics are possible under the STA.

- c. What activities at your agencies are covered by the STA?**

None at OSTP.

- d. The academic community has come out in strong support of the STA. To what extent do you believe private research collaboration would be impacted by termination of the STA?**

Private research collaboration should not be directly impacted as the STA supports only government-to-government scientific cooperation.

- e. Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22 USC 6901 note) requires that the Secretary of State "coordinate the activities of all agencies of the United States Government that carry out cooperative activities under the Agreement." Please describe the mechanisms your agencies employ to keep the State Department**

apprised of work your agencies are carrying out pursuant to the STA.

OSTP is not carrying out any work under the STA.

- f. Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22 USC 6901 note) also requires the President to create an interagency working group to oversee the implementation of the STA.**

- i. Dr. Prabhakar, does this working group exist? What are its current functions, scope, and level of activity?**

Yes. This work is currently being led by the National Security Council in collaboration with the State Department. Further information may be shared in an appropriate classified setting.

- ii. Are your agencies part of this working group?**

Yes, OSTP is part of this working group.

- 5. The academic community has demonstrated limited awareness of the range of threats posed by the PRC. What steps or initiatives have your agencies taken over the last year to help make universities and researchers aware of this threat? What has been the response?**

The U.S. government has engaged continuously with academic stakeholders on the range of threats posed by the PRC, and we have seen a steady increase in awareness among academic stakeholders. For instance, the “Statement of the Association of American Universities” entered into the record during this hearing described numerous actions taken by the university community to increase awareness, conduct risk mitigation, provide training, and engage with intelligence agencies and security officials.

OSTP will continue to work to ensure that the academic community has the most relevant and up-to-date information necessary to guard against all threats to the academic research enterprise.

- 6. The Trump Administration’s Department of Justice launched the China Initiative to address the systemic, widespread, and unique threat posed to our national security and way of life by the Chinese Communist Party. It included the development of an enforcement strategy concerning lab researchers at universities. However, the Biden Administration disbanded this initiative, citing “concerns from the civil rights community that [it] fueled a narrative of intolerance and bias.”**

- a. Does the Biden Administration agree that the threat posed to our research base by the CCP is unique in its scope, effectiveness, and penetration?**

The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it. As noted in

his 60 Minutes interview with other Five Eyes intelligence leaders, FBI Director Wray stated, “The People's Republic of China represents the defining threat of this generation this era. There is no country that presents a broader, more comprehensive threat to our ideas, our innovation, our economic security, and ultimately our national security.”

b. Why has the Biden Administration failed to replace the China Initiative with an alternative framework that it does not deem to be problematic?

We understand that the Department of Justice (DOJ) announced the “China Initiative” in 2018, and subsequently replaced that initiative in 2022 with the launch of a Strategy for Countering Nation-State Threats, which takes a more comprehensive approach to addressing illegal activity from hostile nations, including the PRC, Russia, Iran and North Korea. We would refer you to the DOJ for additional information.

c. To your knowledge has the Department of Justice implemented specific strategies to fill the gap left by the termination of the China Initiative?

Please see the response above. We would refer you to the DOJ for additional information. On February 16, 2023, the DOJ and the Department of Commerce announced the creation of the Disruptive Technology Strike Force to prevent nation-adversaries such as the PRC, Iran, Russia, and North Korea from obtaining advanced technologies, including those related to supercomputing, artificial intelligence, quantum computing, advanced manufacturing and materials, and biosciences. The Strike Force consists of sworn agents from the Commerce Department’s Office of Export Enforcement, Federal Bureau of Investigation, Homeland Security Investigations, and Defense Criminal Investigative Service. The Strike Force is currently active in 14 metropolitan regions across the U.S., including Atlanta, Austin, Boston, Chicago, Dallas, Houston, Los Angeles, Miami, New York City, San Jose, Phoenix, Portland, Oregon, Savannah, and Washington, D.C.

7. The CCP does not play by the same rules and standards in the scientific community. For example, the CCP is not transparent and purposely obfuscates its affiliations with its defense research industrial base. Another example is that the PRC has closed access off to their scientific papers to western countries, yet takes advantage of our open basic research papers.

a. What is the Biden Administration’s strategy for naming and shaming the PRC for not playing by universally accepted academic standards?

The U.S. closely coordinates with our allies and partners to draw attention to the PRC’s asymmetric participation in the global research enterprise and its efforts to acquire and outright steal critical emerging technologies. The State Department hosts numerous activities for foreign audiences on these subjects in public and other unclassified settings.

b. In your agencies’ assessment, how would you describe access by U.S. academics and experts to ongoing research activities, projects, symposia, and other scientific and technology activities in China, and how would you

compare this access to such activities in the U.S. enjoyed by PRC researchers?

While the PRC has curtailed access to a number of research areas, including the recent cut-off of foreign access to the Chinese National Knowledge Infrastructure, the share of open access articles in the PRC actually grew from 12 percent in 2012 to 39 percent in 2022, according to the STEM Open Access Dashboard. About 55 percent of all articles from the U.S. are open access today. Though the PRC places strict controls on access to a variety of its facilities, there are unique laboratories in the PRC which remain widely used and are accessible to U.S. and global academics.

Given the nature of ongoing PRC efforts to recruit capital and talent to contribute to significant research and development projects and/or the subsequent cut-off of ties in specific fields of research and development, it is important that the U.S. government continue to monitor the PRC's efforts to engage internationally, particularly with respect to cooperation on technologies or other fields of research relevant to the PRC's military civil fusion efforts.

- 8. The United States has always been a premier destination for foreign academic talent. However, this leaves the United States vulnerable to breaches in research security.**
 - a. What can be done to balance the need to keep the United States as a destination for foreign science and technology talent while protecting American intellectual property?**

OSTP is focused first and foremost on protecting critical and emerging technologies. It is important that we continue to be clear with the broader R&D community about the actual risks associated with technological misappropriation in addition to what we expect from participants in the research enterprise.

- b. In your view, should the United States continue to educate the next generation of PRC STEM students?**

As noted by Secretary Blinken, we continue to welcome students from around the world and are lucky when the best global talent not only studies here but stays here. More than 80 percent of Chinese students who pursue science and technology PhDs in the U.S. choose to stay in the U.S.. According to the National Science Board 2024 Science and Engineering Indicators report, this is higher than the global average of about 70 percent.

- 9. The CCP sees all ethnically Chinese individuals as its subjects, making such individuals top targets for harassment, coercion, and cooption.**
 - a. What steps has the Biden Administration taken to help shield Chinese American academics from CCP harassment or coercion?**

OSTP has been working with the National Security Council to coordinate our research security and foreign malign influence efforts, including communicating with academic associations about the threat of foreign malign influence and transnational repression on campuses. We continue to brief academic organizations on these efforts, in partnership with the National Security Council and the law enforcement and intelligence communities.

- b. What steps has the Biden Administration taken to ensure that academic institutions support their Chinese American employees and students when these employees are faced with such harassment?**

See previous answer.

Rep. Scott Franklin**1. What makes a successful response to mitigating or identifying a research security threat? How do we ensure these successful or unsuccessful responses are properly reported?**

There is no one answer to this question, as there is no single set of characteristics that define a research security violation. For operational security reasons, many of the details concerning these threats must remain classified, but we would be happy to provide further details in an appropriate setting.

Ensuring that violations are properly identified and reported by the academic community requires the provision of specific details about the nature of research security threats, including by providing concrete examples of how certain practices resulted in the improper transfer of information that are clearly harmful to U.S. interests. Such examples are essential in order to ensure that researchers in academia know what to look for. Further, the provision of specific and actionable information is more likely to be accepted by academic faculty and support trust-building with security officials, as academics will inherently be the first line of reporting potential research security concerns or violations.

In June 2022, Assistant Secretary Matthew Axelrod of the Department of Commerce's Bureau of Industry and Security (BIS), announced the creation of the Academic Outreach Initiative (AOI) in order to address the national security risk that foreign adversaries pose to academic research institutions. The AOI has focused on strategic prioritized engagements on academic institutions that possess ties to foreign universities or those who are involved in research and development for the Department of Defense. Further, the AOI has dedicated sworn federal agents who are part of BIS' law enforcement arm, the Office of Export Enforcement, to conduct outreach. OEE agents and analysts within BIS provide background briefings and training to prioritized academic research institutions.

2. What steps are being taken to utilize artificial intelligence, data analytics, or other advanced technologies and methods to ensure the accuracy and completeness of research security disclosures?

The National Science Foundation has developed guidelines for research security analytics using widely-available information, which may be found at: <https://new.nsf.gov/research-security/guidelines>. These guidelines are available for use by all government agencies.

Rep. Brian Babin**1. Does China offer the United States and other foreign nations reciprocal waivers for the export of their foundational research? And if not, why should we maintain this waiver?**

‘Fundamental research’ means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community through scholarly journals or other widely-available datasets. Sharing such information throughout the scholarly community allows for the rapid dissemination of ideas to individuals who can validate, refine, build on, or use it for technological innovation.

As such, there is no waiver process for fundamental research because fundamental research is defined as research that is ordinarily widely shared, and implementing any waiver process would severely inhibit the flow of knowledge in ways that could cripple innovation and have severe consequences for public health and safety.

There are limits to the sharing of fundamental research. Fundamental research that could be used to cause harm may be subject to classification, and information that is not intended to be widely shared may not qualify for the fundamental research exemption of export controls.

As shown in Figure 3 of the November 2023 OSTP “Report to the U.S. Congress on Financing Mechanisms for Open Access Publishing of Federally Funded Research”, in 2021 just under 40 percent of all Chinese publications were made freely accessible without a subscription, compared to about 55 percent of all U.S. research publications. The PRC does, however, place limits on foreign access to certain types of data, resulting in its asymmetrical participation in the global research ecosystem.

Rep. Summer Lee

- 1. How is the OSTP prioritizing workforce development to expand the science & tech workforce through the provision of tools, resources, and funding, especially in underserved/underrepresented communities to sustain/grow federal workforce and address security challenges?**

To protect our national security and ensure our nation's economic and technological competitiveness, OSTP is prioritizing STEM learning and training in a number of ways. One is through NSTC's Committee on STEM (CoSTEM), which coordinates federal agency programs, initiatives, and activities for STEM education, STEM workforce training and development, and STEM research and innovation capacity. CoSTEM is prioritizing creating access and opportunities for our nation's STEM learners, researchers, and workers, with a particular goal of carrying out CHIPS and Science Act provisions that are committed to ensuring our country's full participation in the STEM ecosystem. This includes increasing awareness and access to federal funding and federally funded opportunities, building and sharing the evidence of promising policies and practices, and disseminating federal resources. A new five-year strategic plan is currently in development. OSTP also leads other NSTC committees and initiatives that advance disciplinary-focused areas of the STEM workforce, around the bioeconomy, advanced manufacturing, AI, quantum, microelectronics/ semiconductors, and other critical and emerging areas of technology.

Responses by Dr. Rebecca Keiser

**U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON SCIENCE, SPACE,
AND TECHNOLOGY**

“Examining Federal Science Agency Actions to Secure the U.S. Science and
Technology Enterprise” Dr. Rebecca Keiser, Chief of Research Security Strategy and
Policy, U.S. National Science Foundation

Chairman Frank Lucas

Chairman Lucas Question for the Record for Dr. Keiser

Does NSF ensure that research proposals undergo rigorous scrutiny to evaluate the potential dual-use nature or sensitivity of the research, particularly in technology fields targeted under Military-Civil Fusion such as quantum computing, semiconductors, artificial intelligence, and advanced nuclear technologies?

NSF Response: In NSF’s 2024 Proposal & Award Policies & Procedures Guide (PAPPG), NSF stated that it would be performing assessments of NSF proposals to identify potential national security risks. NSF has developed a draft risk rubric for this assessment. The JASON has “road tested” this rubric and NSF is in the process of doing further assessment. NSF will then pilot the revised rubric on quantum proposals to evaluate effectiveness. Full implementation of the risk rubric to be used on proposals in these sensitive technology areas is expected to occur by the end of calendar year 2024.

Rep. Darrell Issa

Questions for All Witnesses

- 1) For decades, the United States has pursued broad-based research science and technology collaboration with the People's Republic of China, especially between academic institutions in the United States and China's universities.

- a) To what extent does the United States rely upon the PRC's research and development apparatus for our scientific advancement?

NSF Response: The United States relies on its own robust scientific talent base and its unparalleled Federal and private research funding system to perform research. Through efforts such as the NSF Technology Innovation and Partnerships Directorate the U.S. works to translate that research into innovation. The U.S. pursues international partnerships to leverage resources and capabilities from international partners based on the principles of openness, transparency, reciprocity, merit-based competition, and mutual benefit.

- b) Do your agencies assess if this broad-based cooperation continues to be in the United States interest? If so, why?

NSF Response: NSF continually evaluates all of its international partnerships to ensure benefit to the United States. If such benefit cannot be identified, NSF will not continue a partnership.

- c) Are benefits derived from such broad-based cooperation reciprocal to both the United States and the PRC?

NSF Response: Per the previous response, NSF will only pursue reciprocal international collaborations. For instance, NSF collaborates with the Natural Sciences Foundation of China on biodiversity research. This collaboration provides NSF-funded researchers access to vital data and information regarding the Chinese biological ecosystem, thereby benefiting the United States.

- d) PRC nationals make up a sizable number of graduate students in U.S. STEM fields.
i) Is the U.S. domestic research enterprise dependent on individuals from the PRC?

NSF Response: The U.S. domestic research enterprise benefits from the diversity of international talent as well as domestic talent at U.S. universities. For instance, since 2000, 40 percent of U.S. Nobel laureates have been foreign-born. However, the U.S. is not dependent on students from any one particular country.

- ii) Could this talent pool be replaced by nationals from partner countries?

NSF Response: The talent pool needs to continue to be from a diversity of other countries as well as from the United States. As students are admitted to U.S. universities based on merit, universities do not dictate countries of origin.

- e) Given General Secretary Xi Jinping's expansive understanding of "national security" do your agencies assess that research collaboration with the PRC on STEM technologies is inherently dual-use? If not, why not?

NSF Response: NSF is concerned about PRC military-civil fusion efforts and is therefore extremely selective in collaborative programs. Strong benefit to the United States must be identified such as in biodiversity research per the previous response.

- 2) Fundamental research has long been exempt from export controls. Despite significant advances in our understanding of the Chinese Communist Party's technological ambitions and strategy, this policy has yet to be revisited.

- a) Do you believe the time has come to reevaluate National Security Decision Directive 189?

NSF Response: Through NSF's risk assessment efforts, risk mitigation plans can be developed to safeguard research while keeping the research unclassified.

- b) Do your agencies assess that fundamental research is necessary for the PRC to achieve the goals of its Made in China 2025 industrial policy?

NSF Response: NSF respectfully refers this question to other U.S. government agencies that have intelligence capabilities to provide information on the PRC.

- c) Do your agencies assess that basic research collaboration and knowledge transfer of fundamental research support People's Liberation Army modernization?

NSF Response: NSF respectfully refers this question to other U.S. government agencies that have intelligence capabilities to provide information on the PRC.

- d) Can you describe the benefits that would result from stemming the flow of basic research to the PRC?

NSF Response: NSF respectfully refers this question to other U.S. government agencies that have intelligence capabilities to provide information on the PRC.

- 3) Since the China Initiative's termination, have any of your agencies experienced a shift in the willingness or ability of the Justice Department to pursue criminal cases related to research security violations and intellectual property theft from China?

NSF Response: The NSF Office of Inspector General (OIG) informed us that they have not experienced a shift in the willingness or ability of DOJ to pursue criminal cases related to research security since the termination of the China Initiative.

- 4) On November 8, 2023, I led a group of Members in sending a letter to Secretary Blinken, Secretary Raimondo, and Ambassador Tai requesting that they pause negotiations on the U.S.-China Science and Technology Cooperation Agreement (STA).
a) To your knowledge, what is the status of STA renewal negotiations?

NSF Response: NSF respectfully refers this question to the U.S. Department of State who is leading these negotiations.

- b) Do your agencies assess that the United States derives reciprocal or substantial benefits from maintaining a broad-based research cooperation agreement with the PRC rather than specific agreements on discrete topics, such as influenza?

NSF Response: STAs provide a framework for government-to-government cooperation by stating expectations, setting guardrails, and furthering consistency in approach, while allowing flexibility to engage in cooperation on discrete topics through other arrangements (MOUs, Protocols, etc.).

- c) What activities at your agencies are covered by the STA?

NSF Response: NSF has long-standing cooperation with three joint funding programs with the National Natural Science Foundation of China (NSFC) via a 1995 Protocol and 2006 Memorandum of Agreement on Cooperation in the Basic Sciences, both of which are under the STA. In these programs, NSF funds are provided to U.S. institutions to support U.S. researchers, and NSFC funds the Chinese side of the collaborative projects.

- d) The academic community has come out in strong support of the STA. To what extent do you believe private research collaboration would be impacted by termination of the STA?

NSF Response: STAs facilitate government-to-government cooperation. NSF understands that the academic community pays close attention to the words and actions of the U.S. government vis-a-vis the People's Republic of China, however, private research is not directly impacted by the U.S.-PRC STA.

- e) Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22 USC 6901 note) requires that the Secretary of State “coordinate the activities of all agencies of the United States Government that carry out cooperative activities under the Agreement.” Please describe the mechanisms your agencies employ to keep the State Department apprised of work your agencies are carrying out pursuant to the STA.

NSF Response: NSF works collaboratively with the State Department to provide relevant information regarding activities with the People's Republic of China in a timely manner.

- f) Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22 USC 6901 note) also requires the President to create an interagency working group to oversee the implementation of the STA.
- i) Does this working group exist? What are its current functions, scope, and level of activity?

NSF Response: NSF attends interagency meetings as appropriate if/when they are called by the State Department or the National Security Council. We respectfully refer you to the State Department or the National Security Council for additional details.

- ii) Are your agencies part of this working group?

NSF Response: NSF attends interagency meetings as appropriate if/when they are called by the State Department or the National Security Council.

- 5) The academic community has demonstrated limited awareness of the range of threats posed by the PRC. What steps or initiatives have your agencies taken over the last year to help make universities and researchers aware of this threat? What has been the response?

NSF Response: NSF believes that the US Government needs to work together with the academic community to create a research security culture. NSF has accomplished the following efforts in raising awareness at universities and with researchers:

- Research security training modules: NSF co-funded four training modules with the Department of Energy, National Institutes of Health, and Department of Defense that were released broadly to the community in January 2024. These modules are intended to assist the community in fulfilling the training requirement outlined in P.L. 117-167, commonly known as the CHIPS and Science Act. Community feedback on the modules has been extremely favorable.
- SECURE Center: NSF has completed the solicitation for the SECURE Center and is in the process of finalizing the award. As outlined in CHIPS and Science, SECURE will provide the community with the tools, resources, and services to empower them to address research security and integrity issues.

- NSF Office of the Chief of Research Security Strategy and Policy: NSF is finalizing the addition of two staff and has also brought on three full time contractors to the existing 5-person team in order to scale up its research security analytics efforts and enhance its communication efforts with the community.
- Research on Research Security (RoRS): NSF will hold a RoRS workshop this summer to form a community of practice to further understand and explore research security issues through research projects implemented by the community.
- Domestic and international outreach: NSF uses its close partnership with university associations, scientific societies, and research institutions to meet regularly and visit institutions to communicate and discuss research security issues.

NSF has found a greatly increased understanding of these issues at universities and by researchers, as demonstrated by the frequent proactive provision of corrected disclosure information from universities to NSF and the establishment of research security and risk assessment processes at many universities.

- 6) Criminal charges against college and university professors currently comprise only 3 percent of all economic espionage prosecutions. However, there is growing cases of grant fraud at federal research agencies and universities associated with China.
- a) Can you please elaborate on how your office's caseload of research security cases has changed over the last 2 years?

NSF Response: The NSF OIG informed us that Research Security cases, as a percentage of open civil/criminal investigations, has decreased from 57% of such cases in March 2022 to 30% of such cases in March 2024. Factors affecting this change include bringing existing research security cases to a conclusion during that two-year period and receiving fewer research security allegations through the OIG hotline and other sources.

- b) Is your office proactively pursuing such cases? Why or why not?

NSF Response: The NSF OIG informed us that it currently has an open proactive review addressing unreported foreign gifts to American universities, which has led to one civil settlement as of March 2024. The NSF OIG continues to investigate allegations of research security-related grant fraud and participates in joint investigations of such matters initiated by other OIGs when NSF OIG has an appropriate nexus. Finally, NSF OIG continues to lead an OIG community working group focused on research security which fosters relevant training, cross-OIG information sharing, and investigative collaborations.

Rep. Scott Franklin**Rep. Scott Franklin Questions for the Record:**

What makes a successful response to mitigating or identifying a research security threat? How do we ensure these successful or unsuccessful responses are properly reported?

NSF Response: NSF is working with the research community to create a research security culture. Ideally, as this culture is created, research institutions will be able to identify and mitigate a research security threat prior to an issue being raised by the U.S. government. NSF will provide services to the community through the Safeguarding the Entire Community in the U.S. Research Ecosystem (SECURE) Center. SECURE will provide tools, information, and services to the community to assist them in identifying and mitigating such risks. NSF anticipates the SECURE Center awardee will be announced summer 2024.

What steps are being taken to utilize artificial intelligence, data analytics, or other advanced technologies and methods to ensure the accuracy and completeness of research security disclosures?

NSF Response: NSF has developed a robust analytics tool that assesses information provided to NSF through disclosures with large databases to identify inconsistencies in reported affiliations, sources of funding, patents, and other information. NSF uses this information to focus on research security risks. NSF has made its [research security analytics guidelines](#) public and has also hired three full-time contractors to implement these analytics as well as a full-time civil servant senior data advisor.

This Committee has heard from researchers that they are blamed when identifying foreign threats, as it reveals a weakness in their security systems. How can federal science agencies sincerely protect and support our researchers to address vulnerabilities without impacting their strength to identify threats?

NSF Response: As part of NSPM-33, institutions will be required to establish research security programs. The SECURE Center will be a non-governmental organization through which researchers will also be able to report threats and concerns.

Can you please speak to how NSF is or is not meeting its research security goal to improve disclosure requirement transparency, and mitigating risks of security threats? How do you clearly quantify success in these areas, outside of hosting webinars?

NSF Response: NSF is pleased that the common forms for disclosure have been finalized and each Federal Agency is in the process of implementing these common forms. Through this effort, disclosure requirement transparency will be greatly enhanced. Through NSF's research security analytics efforts, NSF will be able to monitor the success of this disclosure transparency. Success will be quantified if the rate of disclosure inconsistencies decreases. Additionally, through the SECURE Center, research security threats can be identified and mitigated. The SECURE Center is required to include an evaluation effort so that success of the Center's efforts can be measured.

Rep. Brian Babin

Rep. Brian Babin Question for the Record:

The CHIPS and Science Act authorized the establishment of a computing enclave pilot program. This was 18 months ago. Can you please provide an update on the status of this program?

NSF Response: NSF is taking a multi-pronged approach to piloting computing enclaves through cyberinfrastructure investments that can facilitate regulated and sensitive research at U.S. Institutions. The Office of Advanced Cyberinfrastructure (OAC)¹ within the Computer and Information Science and Engineering (CISE) directorate is supporting training and expertise; development, deployment, and experimentation; and basic research in secure enclaves. A notable initiative within CISE/OAC includes the Cybersecurity Innovation for Cyberinfrastructure (CICI) program², which has supported:

Training, expertise, and best practices:

- The Regulated Research Community of Practice (RRCoP)³ to build the requisite expertise among University IT and research computing administrators; NSF award 2409859.⁴
- The NSF Trusted CI Cybersecurity Center of Excellence⁵ (NSF award 2241313⁶) provides tailored engagements with large NSF facilities and research projects, including technical and policy advice on building and maintaining secure enclaves. For example, Trusted CI engaged with UC Berkeley in reviewing their Secure Research Data and Compute Platform.⁷
- Development of Purdue's REED+ Secure Research Ecosystem that built a framework for campus best practices in protecting Controlled Unclassified Information or "CUI" research data and integrating NIST SP 800-171 requirements;⁸ NSF award 1840043.⁹
- A joint NSF and NIST High-Performance Computing (HPC) Cybersecurity Workshop in 2023¹⁰ with a planned follow-on workshop in 2024.¹¹

Experimental deployments:

- A state of Virginia-wide research computing enclave, "ACCORD," as part of the NSF Major Research Instrumentation (MRI) program; NSF award 1919667.¹²

¹ <https://new.nsf.gov/cise/oac>

² <https://new.nsf.gov/funding/opportunities/cybersecurity-innovation-cyberinfrastructure-cici>

³ <https://www.regulatedresearch.org/>

⁴ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2409859

⁵ <https://www.trustedci.org/>

⁶ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2241313

⁷ <https://scholarworks.iu.edu/iu-swrrest/api/core/bitstreams/36ef78f5-746a-45de-9f8b-g9228b0edfe0/content>

⁸ <https://www.rcac.purdue.edu/services/reedplus>

⁹ https://www.nsf.gov/awardsearch/showAward?AWD_ID=1840043

¹⁰ <https://csrc.nist.gov/pubs/ir/8476/final>

¹¹ <https://hpcc.okstate.edu/oak-consortium.html>

¹² https://www.nsf.gov/awardsearch/showAward?AWD_ID=1919667

- Privacy-enhancing technology deployment within ACCORD; NSF award 2319988.¹³
- The SOTERIA secure open science container archive that provides curated and vetted collections of important science software applications; NSF award 2115148.¹⁴
- The University of New Mexico's SAMPRA secure enclave; NSF award 1840069.¹⁵

Foundational Research:

- Development of isolation technologies within High-Performance Computing as a mechanism to support more secure enclaves; NSF award 2319975.¹⁶
- Enabling and supporting efficient large, distributed computation using hardware isolation primitives. Such primitives are a prerequisite to supporting MapReduce-type workloads in secure enclaves; NSF award 2232824.¹⁷
- Enabling secure, privacy-preserving queries of massive science datasets; NSF award 2232813.¹⁸
- The UC Irvine Horizon secure hypervisor that provides improved security guarantees for privacy sensitive data and computing in the cloud; NSF award 1840197.¹⁹

NSF will continue to support efforts to enhance the security of research data and assist institutions and researchers with safeguarding regulated and sensitive information.

¹³ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2319988

¹⁴ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2115148

¹⁵ https://www.nsf.gov/awardsearch/showAward?AWD_ID=1840069

¹⁶ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2319975

¹⁷ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2232824

¹⁸ https://www.nsf.gov/awardsearch/showAward?AWD_ID=2232813

¹⁹ https://www.nsf.gov/awardsearch/showAward?AWD_ID=1840197

Responses by Dr. Geri Richmond

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

QUESTIONS FROM CHAIRMAN FRANK LUCAS

- Q1. The Exascale Computing Project has been a resounding success with the Frontier supercomputer, located in my district at Oak Ridge National Laboratory, and the Aurora supercomputer being brought online to be the two most powerful ever. However, this project is winding down, Dr. Richmond, what is DOE doing to prepare for what comes after these Exascale computers to ensure that we secure our commanding position in advanced computing?
- A1. Building on the success of the Exascale Computing Project (ECP), the Department has initiated strategic investments to maintain U.S. leadership in advanced computing. The Department has established the mission need for upgrades to the Leadership Computing Facilities (LCF) and the national laboratories have engaged the vendor community to understand what technologies are likely to be available for these systems. Oak Ridge National Laboratory (ORNL) will soon issue a Request for Proposals for cost-shared collaborative research, called Next Frontiers, aimed at enhancing advanced computing technologies to better address the scientific and engineering challenges of the Department (see <https://www.olcf.ornl.gov/draft-olcf-6-technical-requirements/>). These efforts are the first in a series of engagements that are patterned after the very successful ECP vendor partnerships.

In addition, the Department is transitioning the ECP software ecosystem into a community-led High Performance Software Foundation, that can merge continued improvements from the vendors, facilities, and the research community under the structure of the successful open source Linux foundation. The Department is also investing in a wide array of Artificial Intelligence capabilities that are advancing application performance on the existing Exascale systems as well as planned upgrade systems. In parallel, the Department continues to invest in Quantum Information Science (QIS) testbeds, algorithms, and applications in anticipation of future HPC systems capable of harnessing quantum accelerators.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

Driving energy-efficient innovation at every level of the HPC system remains a paramount strategic objective for DOE. Over the past ten years, the DOE National Laboratories and the HPC vendor community have been integrating and co-designing energy efficient solutions, from the individual devices in supercomputers to the high-capability computing centers that house and power them. As computing architectures become more hybrid with multiple diverse accelerator technologies at play, DOE must continue its leadership in energy efficiency while advancing the state of the art in compute capability in simulation, AI, and quantum. DOE has already initiated modest investments in energy-efficient computing to cover a broad range of technology areas in compute, memory, networking, and storage aligned with the National Science and Technology Council’s (NSTC) Advanced Computing Ecosystem Strategic Plan. DOE’s holistic approach, including basic-research, testbeds, industry partnerships, and first-of-a-kind deployments, is essential to feeding the innovation pipeline for both DOE’s use cases and the CHIPS programs. DOE is also an essential contributor of compute capability to the National AI Research Resource Pilot, which aims to democratize access to compute resources across the nation’s research community.

- Q2. How is DOE leveraging the National Laboratory Complex to educate and collaborate with university researchers so that they have a better understanding of research security?
- A2. Several DOE national laboratory directors and senior laboratory personnel serve and engage on the National Academies of Sciences, Engineering, and Medicine (NASEM) National Science, Technology, and Security Roundtable. Some sessions of these roundtables have specifically focused on the cross-section of academic institutions and research security. Through this engagement, best practices have been shared by the laboratories in how best to implement research security policies while also ensuring an open and collaborative scientific ecosystem.

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

Additionally, DOE has pursued several forms of engagement and outreach to the research and academic communities to both communicate research security policies as well as address questions and concerns. The response by the community has been very positive.

- As a co-chair of the National Science and Technology Council (NSTC) Subcommittee on Research Security, DOE has participated in 14 community listening sessions to understand both the concerns surrounding and the impacts of NSPM-33 implementation on the research community. Hosted by the NSTC Subcommittee, these were attended by the S&T funding agencies and universities/advocacy groups in summer 2022.
- DOE partnered with the National Science Foundation (NSF), National Institutes of Health, and Department of Defense to co-fund and support the creation of research security training modules that can serve as an information source and provide best practices to optimize research security. The completed modules are stewarded by NSF and can be found at <https://new.nsf.gov/news/nsf-research-security-training-modules>
- DOE has increased engagement with the academic community through discussions involving the Federal Demonstration Partnership, Council on Governmental Relations, Association of American Universities, the Association of Public and Land-Grant Universities, as well as organizations representing the Asian American, Native Hawaiian, and Pacific Islander research community.
- DOE recently released an unclassified Science and Technology (S&T) Risk Matrix that has been broadly disseminated within the national laboratories and to university partners in order to broaden research security awareness within academic institutions.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

- Q3. With DOE’s introduction of the risk matrix in 2018 how have you worked with other agencies in sharing best practices and lessons learned with that implementation?
- A3. In addition to the activities described above, DOE has broadly shared the best practices and lessons learned from developing the S&T Risk Matrix. A key approach to striking a policy of promote and protect has been *(i)* providing the opportunity for the national laboratory scientific community to identify what is most important in emerging research technology areas and *(ii)* developing additional protections to prevent the premature release of yet-to-be-published research findings. This opportunity for the national laboratory scientific community to help craft reasonable policies has led to the institutionalization of the S&T Risk Matrix as a tool for risk mitigation.

Further, the process for developing the S&T Risk Matrix – scientists engaging fellow scientists – led to greater awareness of research security within the laboratory scientific community. This has also led to broader research security training within the laboratory complex. The Chief Research Officers effectively served as ambassadors for the Department on our concerns, which led to greater acceptance by the laboratory scientific community.

In 2023, the S&T Risk Matrix was updated for the first time since its inception and issued to the national laboratory complex.

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

QUESTION FROM CONGRESSMAN DARRELL ISSA

- Q1. For decades, the United States has pursued broad-based research science and technology collaboration with the People’s Republic of China, especially between academic institutions in the United States and China’s universities.
- Q1a. To what extent does the United States rely upon the PRC’s research and development apparatus for our scientific advancement?
- A1a. The United States relies on its own robust scientific talent base and its unparalleled Federal and private research funding system to perform research. DOE pursues international partnerships and participates in multilateral scientific engagements when deemed necessary to support DOE’s mission and benefit the American people.
- Q1b. Do your agencies assess if this broad-based cooperation continues to be in the United States interest? If so, why?
- A1b. DOE carefully evaluates collaboration with any foreign nation to ensure it is in our interest and more broadly, in the interest of the United States. We carefully evaluate any current and potential future collaboration opportunities that could be in the interest of the United States.

DOE’s international cooperation activities align with Administration strategic priorities; are undertaken for peaceful purposes; bolster U.S. competitiveness in science; have strong intellectual property rights provisions; espouse U.S. values of openness and transparency; and require parity in intellectual and financial contributions from all partners. Many of the external scientific advisory boards that provide guidance to our scientific programs have evaluated and expressed support for DOE supported international projects.

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

- Q1c. Are benefits derived from such broad-based cooperation reciprocal to both the United States and the PRC?
- A1c. DOE takes a very thoughtful and careful approach to any cooperation with the PRC to ensure any collaboration is in the interest of DOE and the United States.
- Q1d. PRC nationals make up a sizable number of graduate students in U.S. STEM fields. Is the U.S. domestic research enterprise dependent on individuals from the PRC? Could this talent pool be replaced by nationals from partner countries?
- A1d. It is widely recognized that a significant portion of the graduate students in U.S. STEM fields are born in other countries. Our understanding is that many of these graduate students choose to stay in the U.S. and contribute to our nation’s STEM enterprise, benefitting U.S. economic growth and intellectual and technological competitiveness. STEM students from a diversity of countries are admitted to U.S. graduate programs on the basis of merit.
- Q1e. Given General Secretary Xi Jinping’s expansive understanding of “national security” do your agencies assess that research collaboration with the PRC on STEM technologies is inherently dual-use? If not, why not?
- A1e. DOE is concerned about PRC military-civil fusion efforts and is therefore extremely selective in the collaborations we pursue with the PRC. DOE’s S&T Risk Matrix requires determining where there is a mutual or net gain for the U.S. in collaborating with countries such as the PRC. Areas where there is not a U.S. or mutual gain are designated as restricted. The Department is extremely thoughtful in areas we collaborate with the PRC with US interests taking primacy.

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

- Q2. Fundamental research has long been exempt from export controls. Despite significant advances in our understanding of the Chinese Communist Party’s technological ambitions and strategy, this policy has yet to be revisited.
- Q2a. Do you believe the time has come to reevaluate National Security Decision Directive 189?
- A2a. DOE recognizes that the actions of the Chinese Communist Party, as well as those of certain other foreign governments, pose significant risks to the research, technology, and economic security (RTES) of the DOE enterprise. For that reason, DOE is actively managing RTES risks while maintaining an open, collaborative, and world-leading scientific enterprise. Towards this end, DOE is implementing nuanced and balanced approaches to combat competitor nations from exploiting our open systems. Recent actions include (a) enhancing existing due diligence processes to ensure that risks of undue foreign influence are considered early in the competitive process and throughout the life of a DOE supported project or loan; (b) establishing a department-wide RTES policy working group to review, develop, and assist in the implementation of RTES policies; and (c) establishing a new RTES Office to implement and continue to evolve DOE’s enhanced due diligence process for financial assistance and loan projects, build awareness internally within DOE on RTES issues, engage with external stakeholders, and assist in the review of DOE national lab agreements involving foreign entities. These efforts will complement and enhance already-existing RTES policies, procedures and tools used to mitigate risk across the DOE enterprise and national laboratories, including *e.g.*, the Department’s Science and Technology Risk Matrix.
- Q2b. Do your agencies assess that fundamental research is necessary for the PRC to achieve the goals of its Made in China 2025 industrial policy?
- A2b. Open and collaborative fundamental research serves to advance science in the U.S. and other nations. At the same time, certain aspects of fundamental research may be exploited by foreign adversaries for anti-competitive interests, which is why it is

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

important to protect U.S. interests in fundamental research, maintain openness, and successfully compete in the global marketplace for science talent.

- Q2c. Do your agencies assess that basic research collaboration and knowledge transfer of fundamental research support People’s Liberation Army modernization?
- A2c. DOE limits collaboration with the PRC to areas that both benefit DOE and the United States and are of low risk to advancing the modernization goals of the People’s Liberation Army (PLA).
- Q2d. Can you describe the benefits that would result from stemming the flow of basic research to the PRC?
- A2d. Cutting off DOE’s basic research engagement with the PRC could result in a net loss to U.S. economic and technological competitiveness. For example, DOE and the U.S. has benefited from having access to a superconducting tokamak, which we don’t have in the U.S. DOE is thoughtful about the areas in which we cooperate with the PRC, to include areas identified as basic research. Risk assessment tools such as the S&T Risk Matrix serve as guides for determining where collaboration is in the U.S. national interest.
- Q3. Since the China Initiative’s termination, have any of your agencies experienced a shift in the willingness or ability of the Justice Department to pursue criminal cases related to research security violations and intellectual property theft from China?
- A3. From DOE’s perspective, the termination of the China Initiative has not made a noticeable difference in how the U.S. government has approached potential or actual criminal conduct and cases.
- Q4. On November 8, 2023, I led a group of Members in sending a letter to Secretary Blinken, Secretary Raimondo, and Ambassador Tai requesting that they pause negotiations on the U.S.-China Science and Technology Cooperation Agreement (STA).

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

- Q4a. To your knowledge, what is the status of STA renewal negotiations?
- A4a. DOE refers you to the State Department, which leads on STA negotiations.
- Q4b. Do your agencies assess that the United States derives reciprocal or substantial benefits from maintaining a broad-based research cooperation agreement with the PRC rather than specific agreements on discrete topics, such as influenza?
- A4b. The Department of Energy typically engages in collaboration with other countries through the use of international implementing arrangements that are subsidiary to STAs. The broad-based STAs are useful for fundamental research projects since they include clauses related to intellectual property that are negotiated once and can then be applied to each subsidiary arrangement. At the same time, we recognize that the existence of an STA does not convey an explicit expectation for collaboration. Therefore, it is beneficial to have the STA with the PRC since we do not have to collaborate if we do not want to, but could do so if it is deemed in our interest. STAs provide a helpful framework for cooperation by stating expectations, ensuring a consistent USG approach, and allowing flexibility to engage in cooperation through other agreements.
- Q4c. What activities at your agencies are covered by the STA?
- A4c. The Department of Energy has limited collaboration with the PRC.
- Q4d. The academic community has come out in strong support of the STA. To what extent do you believe private research collaboration would be impacted by termination of the STA?
- A4d. Legally, the STA applies only to government-to-government cooperation. DOE does not know how the termination of the STA might impact private research collaboration.
- Q4e. Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22USC 6901 note) requires that the Secretary of State “coordinate the activities

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

of all agencies of the United States Government that carry out cooperative activities under the Agreement.” Please describe the mechanisms your agencies employ to keep the State Department apprised of work your agencies are carrying out pursuant to the STA.

- A4e. DOE regularly shares information with the State Department on our limited collaboration with the PRC.
- Q4f. Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22USC 6901 note) also requires the President to create an interagency working group to oversee the implementation of the STA.
- Q4fa. Does this working group exist? What are its current functions, scope, and level of activity?
- Q4fb. Are your agencies part of this working group?
- A4fa. Yes, this working group exists. However, it is not led by the U.S. Department of Energy (DOE). For further information on its functions, scope, and level of activity, we refer you to the State Department and National Security Council.
- A4fb. Yes, the DOE is an active member on this working group.
- Q5. The academic community has demonstrated limited awareness of the range of threats posed by the PRC. What steps or initiatives have your agencies taken over the last year to help make universities and researchers aware of this threat? What has been the response?
- A5. DOE has pursued several forms of engagement and outreach to the research and academic communities to both communicate research security policies as well as address questions and concerns. The response by the community has been very positive.
- As a co-chair of the National Science and Technology Council Subcommittee on Research Security, DOE has participated in several community listening sessions to understand both concerns surrounding and the impacts of NSPM-33 implementation on the research community.

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

- DOE has increased engagement with the academic community through discussions involving the Federal Demonstration Partnership, Council on Governmental Relations, Association of American Universities, the Association of Public and Land-Grant Universities, as well as organizations representing the Asian American, Native Hawaiian, and Pacific Islander research community. Furthermore, DOE has engaged the academic community through its participation in the National Science, Technology, and Security Roundtable that is organized by the National Academies of Sciences, Engineering, and Medicine.
- DOE partnered with the National Science Foundation (NSF), National Institutes of Health, and Department of Defense to co-fund and support the creation of research security training modules that can serve as an information source and provide best practices to optimize research security. The completed modules are stewarded by NSF and can be found at <https://new.nsf.gov/news/nsf-research-security-training-modules>

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

QUESTION FROM CONGRESSMAN SCOTT FRANKLIN

- Q1. What makes a successful response to mitigating or identifying a research security threat? How do we ensure these successful or unsuccessful responses are properly reported?
- A1. Effective research security measures result from a consistent, coordinated government approach that includes clear policy and guidance coupled with active stakeholder engagement. Strong two-way communication between the government and research and academic communities helps to better clarify and understand threat behaviors, maximize dialogue on expectations and requirements, and build rapport and trust. These partnerships, in turn, allow for the most successful environment to address research security threats. Further, our goal is to continue to raise the level of awareness within research institutions where they identify and take mitigating action on their own when research security issues are identified.
- Q2. What steps are being taken to utilize artificial intelligence, data analytics, or other advanced technologies and methods to ensure the accuracy and completeness of research security disclosures?
- A2. It is essential that federal research funding agencies ensure the accuracy and completeness of disclosures related to the potential conflicts of interest and commitment of participants in the Federally funded R&D enterprise. To complement and expand upon existing policies, procedures, and tools, DOE has established a new Research, Technology, and Economic Security (RTES) Office to implement and continue to evolve DOE’s enhanced due diligence process for financial assistance and loan projects, as well as a department-wide RTES Policy Working Group to review, develop, and assist in the implementation of RTES policies. These groups will continue to evaluate the technology and tools needed to ensure the accuracy and completeness of RTES disclosures. To protect the rights of individuals, implementation of artificial intelligence, data analytics, or other advanced technologies and methods will be implemented in manner consistent with

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy

Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management
for Agency Use of Artificial Intelligence.*

**U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
“Examining Federal Science Agency Actions to Secure the
U.S. Science and Technology Enterprise” Hearing on February 15, 2024
The Honorable Geri Richmond, Under Secretary
for Science and Innovation, Department of Energy**

QUESTION FROM CONGRESSWOMAN SUMMER LEE

- Q1. Western Pennsylvania is one of the nation’s premier ecosystems for robotics, the autonomy sector, and biomanufacturing, but cannot remain so without federal support and investment. How is the Dept. of Energy prioritizing implementation of provisions in the CHIPS & Science Act support to academic institutions and business entities in addressing security risks to research?
- A1. The DOE created the Science and Technology (S&T) Risk Matrix in 2019. In 2023, the S&T Risk Matrix was updated for the first time since its inception and issued to the national laboratory complex. An unclassified S&T Risk Matrix has been disseminated to the national laboratories, university partners and shared with our partner science funding agencies.

*Responses by Dr. Michael Lauer*U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY*“Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise”*

Dr. Michael Lauer, Deputy Director for Extramural Research, National Institutes of Health

Chairman Lucas Question for the Record for Dr. Lauer:

This Committee has heard from stakeholders that the Chinese Communist Party (CCP), through third-party entities, is actively submitting FOIA requests against us. How can federal science agencies, or academic institutions for that matter, address this security threat?

NIH Response:

Under the law, there are few limitations on who can file a FOIA request, nor can an agency's response to a request vary depending on its provenance. Any individual, partnership, corporation, association, or public or private organization, other than a Federal agency, regardless of nationality, may submit a FOIA request to HHS. NIH is aware that a small portion of the incoming FOIA requests emanate directly from China, but cannot ascertain which requests emanate indirectly from that country: it is easy to obfuscate the source of a FOIA request, as that information is self-reported by the requester. As an initial matter, the NIH FOIA program is constantly vigilant about the potential release of protected information, e.g., Trade Secrets, Confidential Commercial information, Personal Privacy information, and internal deliberations the release of which would cause foreseeable harm or are prohibited from release. For example, under section 2013 of the 21st Century Cures Act (Public Law 114-255), HHS (including NIH) may exempt from disclosure under FOIA any biomedical information about an individual that is gathered or used during the course of biomedical research if the individual is identified or there is at least a very small risk that their identity could be deduced. In the context of confidential commercial information, the agency will reach out to the enterprises that submitted the information for their input on what they consider to be exempt from disclosure under the FOIA. On occasion, these enterprises have responded to our outreach expressing concern that the incoming request was from an entity in China. However, the government's responsibilities under FOIA are not drawn to distinguish the provenance of requests, nor has the NIH FOIA program received guidance that requests should be treated differently in response to a particular requester or any particular security threat. Consequently, we continue to process FOIA requests in accordance with our regulations and to withhold information where disclosure would either foreseeably harm an interest protected by a FOIA exemption or disclosure is prohibited by law.

Rep. Darrell Issa Questions for the Record:

Questions for All Witnesses:

1. For decades, the United States has pursued broad-based research science and technology collaboration with the People's Republic of China, especially between academic institutions in the United States and China's universities.

a. To what extent does the United States rely upon the PRC's research and development apparatus for our scientific advancement?

NIH Response:

We would be happy to provide information along these lines in an appropriately classified setting..

b. Do your agencies assess if this broad-based cooperation continues to be in the United States interest? If so, why?

NIH Response:

The PRC is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do so. This means that we must be selective in the areas in which the U.S. government collaborates with PRC entities and that we continue to demand adherence to norms of transparency and reciprocity that underpin the global research enterprise.

As the PRC's scientific capabilities increase, so too does the United States' need to have a thorough understanding of the PRC's capabilities. This requires some degree of scientific interaction, the overwhelming majority of which is outside the control of the federal government.

Similarly, the PRC's efforts to increase its interests in multilateral technical fora require constant U.S. attention and engagement to ensure that we can strengthen and maintain the normative frameworks that underpin the global research enterprise. Consistent with the National Security Strategy, this allows us to align our efforts with our network of allies and partners, acting with common purpose and in common cause, and compete responsibly with the PRC to defend our interests and build our vision for the future..

c. Are benefits derived from such broad-based cooperation reciprocal to both the United States and the PRC?

NIH Response:

This depends on the field of research. In an increasing number of areas, PRC data laws and the vagueness of how they are implemented have made it increasingly difficult to engage in transparent and reciprocal cooperation with U.S. and global research institutions. As the PRC

becomes a knowledge producer, it is inevitable that gaining access to some of that knowledge through collaborative efforts would be in the U.S. national interest..

d. PRC nationals make up a sizable number of graduate students in U.S. STEM fields.

i. Is the U.S. domestic research enterprise dependent on individuals from the PRC?

ii. Could this talent pool be replaced by nationals from partner countries?

NIH Response:

U.S. biomedical research is not dependent on individuals from any single country. NIH welcomes principled collaborations¹ with foreign nationals, including postdoctoral scholars and graduate students, from across the world. NIH recognizes that their extraordinary contributions to American science are indisputable and the biomedical research workforce continues to be greatly enriched and strengthened by their participation. The research community must find ways to strengthening these important and successful relationships with foreign scientists while simultaneously protecting the Nation's biomedical innovations and intellectual property.

e. Given General Secretary Xi Jinping's expansive understanding of "national security" do your agencies assess that research collaboration with the PRC on STEM technologies is inherently dual-use? If not, why not?

NIH Response:

There is no single answer to this question, particularly given that basic research is defined as research without specific applications towards processes or products in mind. Because of this, it is difficult to characterize all research collaboration as inherently dual use, regardless of the PRC's expansive understanding of national security.

2. Fundamental research has long been exempt from export controls. Despite significant advances in our understanding of the Chinese Communist Party's technological ambitions and strategy, this policy has yet to be revisited.

a. Do you believe the time has come to reevaluate National Security Decision Directive 189?

b. Do your agencies assess that fundamental research is necessary for the PRC to achieve the goals of its Made in China 2025 industrial policy?

c. Do your agencies assess that basic research collaboration and knowledge transfer of fundamental research support People's Liberation Army modernization?

d. Can you describe the benefits that would result from stemming the flow of basic

¹ www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf

research to the PRC?

NIH Response:

NIH refers you to OSTP's response to this same set of questions.

3. Since the China Initiative's termination, have any of your agencies experienced a shift in the willingness or ability of the Justice Department to pursue criminal cases related to research security violations and intellectual property theft from China?

NIH Response:

We maintain a positive working relationship with the Department of Justice (DOJ). It is important to note that NIH's work with the DOJ occurs through the HHS Office of the Inspector General and I am not in a position to comment on deliberations related to potential criminal cases related to research security violations.

4. On November 8, 2023, I led a group of Members in sending a letter to Secretary Blinken, Secretary Raimondo, and Ambassador Tai requesting that they pause negotiations on the U.S.-China Science and Technology Cooperation Agreement (STA).

- a. To your knowledge, what is the status of STA renewal negotiations?
- b. Do your agencies assess that the United States derives reciprocal or substantial benefits from maintaining a broad-based research cooperation agreement with the PRC rather than specific agreements on discrete topics, such as influenza?
- c. What activities at your agencies are covered by the STA?
- d. The academic community has come out in strong support of the STA. To what extent do you believe private research collaboration would be impacted by termination of the STA?
- e. Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22 USC 6901 note) requires that the Secretary of State “coordinate the activities of all agencies of the United States Government that carry out cooperative activities under the Agreement.” Please describe the mechanisms your agencies employ to keep the State Department apprised of work your agencies are carrying out pursuant to the STA.
- f. Section 1207 of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (22 USC 6901 note) also requires the President to create an interagency working group to oversee the implementation of the STA.
 - i. Does this working group exist? What are its current functions, scope, and level of activity?
 - ii. Are your agencies part of this working group?

NIH Response:

This work is currently being led by the National Security Council (NSC) in collaboration with the State Department. Further information may be shared in an appropriate classified setting.

5. The academic community has demonstrated limited awareness of the range of threats posed by the PRC. What steps or initiatives have your agencies taken over the last year to help make universities and researchers aware of this threat? What has been the response?

NIH Response:

Over the last several years, NIH has continued outreach to institutions on the topic of Research Security. Selected examples include:

- Working with the National Science Foundation (NSF) (along with the Department of Defense and Department of Energy) to fund and advise on the development of cooperative agreements that generated four NSF Research Security Training Modules, on the topics of Research Security, Risks, Disclosure Requirements, and International Collaboration. These have received positive feedback from the extramural community.
- Highly involved in the development of common disclosure forms through the White House Office of Science and Technology Policy inter-agency Subcommittee on Research Security, along with development of guidance on malign foreign talent recruitment programs.

- Regular participation in the National Science, Technology, and Security Roundtable Meetings (sponsored by the National Academy of Sciences, Engineering and Medicine) to provide federal agency perspectives on research security.
- NIH's Foreign Interference website includes updated case studies that clearly describe the concerns we are seeing, a description of process for handling allegations and notification, policy information, and more².
- Working closely with individual recipient institutions when research security concerns arise.
- NIH leadership participation in various events at research institutions, including a keynote presentation at Thomas Jefferson University in May 2023 and a Plenary at the Academic Security and Counter-Exploitation Program at Texas A & M University in March 2023.
- Engaging with the Foreign Interference working Group of the Federal Demonstration Partnership, including presenting at their Fall 2023 meeting³.

The response from institutions has been positive. As institutions became more aware of the concerns, self-disclosures from institutions have increased in the last three years. From 2018 to 2019, we received 21 self-disclosures and from 2020-2023 we received 59 self-disclosures.

NIH appreciates the proactive efforts many recipient institutions are taking to comply with these requirements, such as updating institutional disclosure policies, providing outreach to faculty and staff regarding reporting requirements, and initiating reviews to ensure compliance with NIH terms and conditions of award. When instances of noncompliance are identified, NIH works with institutions to help protect the research and research funds.

6. Since it was discovered that the NIH had funded dangerous gain of function research at the Wuhan Institute of Virology, there has been significant concern regarding life sciences collaboration with China. Can you provide the Committee with a comprehensive list of all NIH activities and grants that currently fund activities in China or include significant collaboration with a PRC entity?

NIH Response:

Table 1 reports the active awards as of March 2024 to prime recipient organizations in China. These data were obtained using NIH RePORTER (Research Portfolio Online Reporting Tools Expenditures and Results),⁴ which is a publicly-available electronic tool that allows users to search a repository of both intramural and extramural NIH-funded research projects and related publications and patents resulting from NIH funding.

Table 1. NIH Prime Grant Awards to Recipient Organizations in China

Project Title	Project Number	Prime Organization Name	Fiscal Year
---------------	----------------	-------------------------	-------------

² <https://grants.nih.gov/policy/foreign-interference/about-foreign-interference>

<https://thefdp.org/wp-content/uploads/FIWG-FINAL-NSPM-33-CHIPS-and-Research-Security-Sept-2023-V10.pdf>

⁴ reporter.nih.gov/

China Health and Retirement Longitudinal study	5R01AG037031-13	PEKING UNIVERSITY	2023
Antigen discovery for transmission-blocking vaccines in Plasmodium vivax	5R01AI150533-04	CHINA MEDICAL UNIVERSITY	2023
Impacts of Urbanization on Vector Biology and Transmission of Dengue in China	5R01AI136850-09	SOUTHERN MEDICAL UNIVERSITY	2022

Table 2 reports NIH grant awards and a contract as of March 2024 to primary recipients, and the subaward/subcontract for research/activities conducted in China provided by that primary recipient. Subaward data was obtained from USASpending,⁵ the official open data source of federal spending information, including information about federal awards such as contracts, grants, and loans.

Table 2. Subawards to Recipients in China Made by a NIH Prime Recipient

AWARD TYPE	FY	PRIMARY ORGANIZATION NAME	PROJECT TITLE	GRANT NUMBER	SITE NAME(S)
Subaward	2021	FRED HUTCHINSON CANCER CENTER	Fast and flexible Bayesian phylogenetics via modern machine learning	6R01AI162611-02	
Subaward	2020	DUKE UNIVERSITY	Antibacterial Resistance Leadership Group (ARLG)	3UM1AI104681-08S1	
Subaward	2022	UNIVERSITY OF CONNECTICUT SCH OF MED/DNT	Prevalence of syphilis and other sexually transmitted infections in men and transgender women who have sex with men in Cali, Colombia	3U19AI144177-04S1	
Subaward	2022	UNIVERSITY OF CONNECTICUT SCH OF MED/DNT	A Global Syphilis Vaccine Targeting Outer Membrane Proteins of Treponema pallidum.	3U19AI144177-03	

⁵ www.usaspending.gov/

AWARD TYPE	FY	PRIMARY ORGANIZATION NAME	PROJECT TITLE	GRANT NUMBER	SITE NAME(S)
Subaward	2022	UNIVERSITY OF CALIFORNIA BERKELEY	Novel fluorescent sensors for imaging neuromodulation	5U01NS113358-04	
Subaward	2023	UNIVERSITY OF SOUTHERN CALIFORNIA	Optimization of GPCR-based fluorescent sensors for large-scale multiplexed in vivo imaging of neuromodulation	5U01NS120824-03	
Subaward	2024	UNIVERSITY OF CALIFORNIA LOS ANGELES	Combining Voice and Genetic Information to Detect Heterogeneity in Major Depressive Disorder	5R01MH122569-05	
Subaward	2023	BROAD INSTITUTE, INC.	Potentiate Cav3.3 To Treat Cognitive Deficits Associated with Impaired Sleep Spindle	3R01MH131719-02	
Subaward	2021	UNIVERSITY OF CONNECTICUT SCH OF MED/DNT	A Global Syphilis Vaccine Targeting Outer Membrane Proteins of Treponema pallidum.	3U19AI144177-02	
Subaward	2024	BROAD INSTITUTE, INC.	Potentiate Cav3.3 To Treat Cognitive Deficits Associated with Impaired Sleep Spindle	5R01MH131719-03	
Subaward	2022	UNIVERSITY OF SOUTHERN CALIFORNIA	Optimization of GPCR-based fluorescent sensors for	5U01NS120824-02	

AWARD TYPE	FY	PRIMARY ORGANIZATION NAME	PROJECT TITLE	GRANT NUMBER	SITE NAME(S)
			large-scale multiplexed in vivo imaging of neuromodulation		
Contract		CANCER HOSPITAL, CHINESE ACADEMY OF MEDICAL SCIENCES		75N91022C00059	CANCER HOSPITAL, CHINESE ACADEMY OF MEDICAL SCIENCES
Subcontract		ICAHN SCHOOL OF MEDICINE AT MOUNT SINAI		75N93021C00014	GUANGXI UNIVERSITY

Rep. Scott Franklin Questions for the Record:

What makes a successful response to mitigating or identifying a research security threat? How do we ensure these successful or unsuccessful responses are properly reported?

What steps are being taken to utilize artificial intelligence, data analytics, or other advanced technologies and methods to ensure the accuracy and completeness of research security disclosures?

This Committee has heard from researchers that they are blamed when identifying foreign threats, as it reveals a weakness in their security systems. How can federal science agencies sincerely protect and support our researchers to address vulnerabilities without impacting their strength to identify threats?

NIH Response:

To ensure proper compliance, NIH has long required the disclosure of all sources of research support, foreign components, and financial conflicts of interest for senior/key personnel on research applications and awards.^{6,7} NIH uses this information when making its funding decisions to determine if the research being proposed is receiving other sources of funding that could be duplicative, appropriate time is committed to the project, or if financial interests may affect objectivity in the conduct of the research.

The number of self-disclosures from institutions rose as institutions became more aware of NIH's concerns⁸. From 2018 to 2019, we received 21 self-disclosures and from 2020-2023 we received 59 self-disclosures. NIH appreciates the proactive efforts many recipient institutions are taking to comply with these requirements, such as updating institutional disclosure policies, providing outreach to faculty and staff regarding reporting requirements, and initiating reviews to ensure compliance with NIH terms and conditions of award. When instances of noncompliance are identified, NIH works with institutions to help protect the research and research funds. If challenges arise with systems at applicant or recipient organizations, NIH will engage with them as appropriate to ensure they are fully aware of what is necessary to ensure proper compliance.

NIH's website explains how the agency handles allegations related to foreign interference.⁹ NIH's administrative/grant compliance review efforts are responsive to objective behaviors, irrespective of the demographics of specific scientists.

NIH employs various strategies to ensure accuracy and completeness of applicant and recipient disclosures. Key amongst these activities involve NIH staff from across NIH who perform grant compliance reviews as part of proper oversight and stewardship of federal awards. This includes Institute/Center program and grants management staff, as well as staff within the NIH Office of Extramural Research. Different electronic tools help compare submitted applications for any potential scientific or budgetary overlap with other applications or funded awards. NIH staff continually test, utilize and employ modern proprietary software and databases, in addition to publicly available information, to gather data used in grant compliance reviews. NIH is actively exploring how to leverage artificial intelligence in several different ways to assess its funded grant portfolio. NIH also collaborates with the National Science Foundation and other federal agencies in these areas, and will continue to

⁶ grants.nih.gov/policy/foreign-interference/requirements-for-disclosure

⁷ grants.nih.gov/grants/guide/notice-files/NOT-OD-19-114.html

⁸ grants.nih.gov/policy/foreign-interference/about-foreign-interference

⁹ grants.nih.gov/policy/foreign-interference/handling-allegations

consider these technologies for ensuring proper oversight, integrity, and accountability for NIH supported research going forward.

If NIH staff determine that an allegation involves NIH-funded research, NIH Office of Extramural Research staff conduct an in-depth assessment (i.e., grants compliance review) to determine whether other support and relevant affiliations were properly disclosed. The NIH Deputy Director of Extramural Research sends a letter to the institution (usually the Vice President of Research) regarding the issue and seeking additional information (including foreign application/grant award documents and foreign employment documents). Institutions typically have between 30-60 days to respond, though these kinds of compliance reviews can be quite complex and lengthy.

The institutional responses are reviewed to assess if any scientific, commitment, or budgetary overlap exists with NIH projects; appropriate disclosure of significant financial interests; adherence to financial conflict of interest management plans; and other factors relevant to the allegation.

NIH will take action and has taken action where appropriate under its authority to address any concerns as part of its proper oversight, compliance, and stewardship roles. As an example, when NIH identifies noncompliance with the terms and conditions of award, it may take actions consistent with the regulatory requirements found in 45 CFR § 75.207 and 45 CFR § 75.371 for grants and FAR 52.227-11 for contracts. Depending on the severity and duration of the noncompliance, NIH may decide to take one or more actions, which are also described in the NIH Grants Policy Statement, Section 8.5, Specific Award Conditions and Remedies for Noncompliance.¹⁰

NIH and the biomedical research enterprise have a long history of international collaborations with rules of engagement that allow science to advance while assuring honesty, transparency, integrity, fair merit-based competition, and protection of intellectual capital and proprietary information. These rules of engagement also are designed to limit bias in the design, conduct, and reporting of NIH-supported research.

NIH expects applicants for and recipients of NIH-supported research — both domestic and foreign — to abide by these principles. It is critical for NIH-supported institutions and their researchers to be wholly transparent about financial support from and affiliations with international institutions. Such transparency ensures that NIH's funding decisions are fair and appropriate, and that U.S. institutions and the American public benefit from their investment in biomedical research. When these expectations for proper transparency, accountability, and stewardship of taxpayer support are met, NIH and the research community will be more successful at mitigating research security concerns.

¹⁰ grants.nih.gov/grants/policy/nihgps/HTML5/section_8/8.5_special_award_conditions_and_remedies_for_noncompliance_special_award_conditions_and_enforcement_actions.htm

Rep. Dale Strong Question for the Record:

Dr. Lauer, many international students take advantage of optional practical training, OPT programs, which allow them to obtain employment in the United States for up to 3 years post-graduation. In 2022 OPT benefited more than 117,000 students with F-1 visas. How can we assist research institutions in coordination of DHS to screen foreign national students and restrict potential bad actors from receiving OPT authorizations?

NIH Response:

This question would best be addressed by the Department of Homeland Security. NIH is not involved in the screenings of foreign national students.

Rep. Summer Lee Questions for the Record:

The genetic material of Henrietta Lacks, taken without consent, has been studied and used globally in major developments on vaccine production, cancer treatments, fertility treatments, and numerous other applications.

How does NIH ensure that individuals and groups involved in the research you conduct are duly aware of the potential uses and outcomes of their contributions to scientific endeavors? What agency do they have over their contributions?

NIH Response:

The NIH Grants Policy Statement, incorporated as a term and condition of all grant awards, stipulates that HHS regulations require recipients to safeguard the rights and welfare of participants in HHS-supported activities (see Section 4.1.15).¹¹ Recipients must obtain a Federal wide Assurance (FWA) with the HHS Office for Human Research Protections (OHRP), and establish appropriate policies and procedures for the protection of human subjects.

In general, HHS regulations require that an investigator obtain the [legally effective informed consent](#) of the subject or the subject's legally authorized representative.¹² Informed consent must be sought prospectively, and documented to the extent required under HHS regulations. The Food and Drug Administration (FDA) regulations at 21 CFR parts 50 and 56 have similar informed consent requirements for clinical investigations that FDA regulates.

The informed consent process generally involves three key features: (1) disclosing to potential research subjects information needed to make an informed decision; (2) facilitating the understanding of what has been disclosed; and (3) promoting the voluntariness of the decision about whether or not to participate in the research. The informed consent process should:

- Be an active process of sharing information between the investigator and the prospective participant
- Ensure that all critical information about a study is completely disclosed, and that prospective subjects or their legally authorized representatives adequately understand the research so that they can make informed choices
- Communicate with the subject population in terms that they can understand
- Provide an opportunity for potential participants to have their questions and concerns addressed on an individual basis
- Be revised when concerns are noted, when new information about reasonably foreseeable risks and potential benefits becomes available, or when other additional information becomes known that will improve the consent process.

The revised Common Rule requires that an IRB-approved version of an informed consent form be posted on a public federal website for all NIH-funded clinical trials.¹³ This must be done after

¹¹ grants.nih.gov/grants/policy/niheps/html5/section_4/4.1.15_human_subjects_protections.htm

¹² <https://www.ecfr.gov/on/2018-07-19/title-45/subtitle-A/subchapter-A/part-46>

¹³ nexus.od.nih.gov/all/2019/06/04/where-to-post-informed-consent-forms-for-nih-funded-clinical-trials/

enrollment ends and within 60 days of the last study visit. This requirement is to make the consent forms being used more transparent and, over time, improve the quality of consent forms. An example of informed consent language for the use of data and biospecimens for secondary research is available on the NIH Scientific Data Sharing website.¹⁴

In addition, all NIH supported and conducted research must follow the requirements for the basic elements of informed consent as specified in the revised Common Rule. As part of these requirements, a statement must be included about any research that involves the collection of identifiable private information or identifiable biospecimens:

- A statement that identifiers might be removed from the identifiable private information or identifiable biospecimens and that, after such removal, the information or biospecimens could be used for future research studies or distributed to another investigator for future research studies without additional informed consent from the subject or the legally authorized representative, if this might be a possibility; or
- A statement that the subject's information or biospecimens collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies.

NIH takes seriously the protection of personally identifiable information, including biological samples and other data, associated with study participants. NIH automatically issues Certificates of Confidentiality as a term and condition of award for applicable human-participant research funded wholly or in part by NIH.¹⁵ These certificates prohibit study participants identifiable, sensitive information from being disclosed except under limited circumstances.¹⁶

Regarding HeLa cells specifically, NIH has taken steps to control access to whole genome sequence data from HeLa cell lines through the establishment and implementation of the 2013 NIH-Lacks Family Agreement,¹⁷ a partnership between NIH and descendants of Mrs. Henrietta Lacks. The Agreement allows biomedical researchers access to HeLa cell whole genome sequence data (HeLa cell data) while also respecting the preferences and privacy of the Lacks family. Under the Agreement, NIH-funded researchers who generate whole genome sequence data from HeLa cell lines are expected to deposit their data into NIH's database of Genotypes and Phenotypes (dbGaP), a controlled-access repository. The HeLa Genome Data Access Working Group¹⁸ of the Advisory Committee to the NIH Director (ACD) assists the ACD in reviewing requests for access to the data, and the ACD makes recommendations to the NIH Director about whether a request should be approved or disapproved. The NIH Director decides whether access to the data will be granted. All researchers seeking access to HeLa cell data are expected to abide by HeLa Genome Data Use Agreement terms.¹⁹

¹⁴ <https://osp.od.nih.gov/wp-content/uploads/Informed-Consent-Resource-for-Secondary-Research-with-Data-and-Biospecimens.pdf>

¹⁵ <https://grants.nih.gov/policy/humansubjects/coc/NIH-funded-Research.htm>

¹⁶ nexus.od.nih.gov/all/2017/09/07/nih-new-certificates-of-confidentiality-policy/

¹⁷ <https://www.nih.gov/news-events/news-releases/nih-lacks-family-reach-understanding-share-genomic-data-hela-cells>

¹⁸ <https://acd.od.nih.gov/working-groups/hlgda.html>

¹⁹ https://dbgap.ncbi.nlm.nih.gov/aa/wga.cgi?view_pdf&stacc=phs000640.v1.pl

In addition, some NIH awards may be subject to the Genomic Data Sharing Policy (GDS Policy),²⁰ effective since 2015. The GDS Policy applies to all NIH-funded research generating large-scale human genomic data and secondary research using these data. It expects consent for research use of human genomic data created or collected after January 25, 2015, and sets expectations for the submission of human genomic data to NIH-designated controlled-access repositories. The GDS Policy also sets standards for secondary use of data according to participant informed consent, with review of research uses by NIH Data Access Committees.

Furthermore, in 2022, NIH released information on Protecting Privacy When Sharing Human Research Participant Data,²¹ to advance efforts under the new Data Management and Sharing Policy (DMS Policy). The information provides a series of principles for protecting privacy, including clear communication of data sharing and use in consent forms. It also recommends a series of best practices for de-identifying research data, establishing data sharing and use agreements, and understanding legal protections against disclosure and misuse of data. Lastly, it recommends sharing sensitive data with controls and to only share data without controls if there is explicit consent from participants and the risks for doing so are very low.

²⁰ <https://www.federalregister.gov/documents/2014/08/28/2014-20385/final-nih-genomic-data-sharing-policy>

²¹ <https://grants.nih.gov/grants/guide/notice-files/NOT-OD-22-213.html>

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD

DOCUMENTS SUBMITTED BY REPRESENTATIVE FRANK LUCAS

Statement of the Association of American Universities

“Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise”

Hearing before the
Committee on Science, Space, and Technology
U.S. House of Representatives

February 15, 2024

The Association of American Universities (AAU), America’s leading research universities, commends the House Committee on Science, Space, and Technology for everything it has done to help bolster the security of federally funded research and to protect against undue foreign influence. We greatly appreciate the committee’s willingness to work with the university and the research community to protect and preserve the scientific openness that has been critical to U.S. leadership in science and technology while at the same time making sure that steps are taken to prevent foreign actors from taking advantage of that openness. We also acknowledge and appreciate the committee’s interest in exercising its oversight role regarding research security and for holding today’s hearing on “*Examining Federal Science Agency Actions to Secure the U.S. Science and Technology Enterprise*.”

America’s leading research universities take seriously both international scientific collaboration and the economic and national security threats posed by foreign adversaries. Theft of intellectual property directly affects universities, which, under the Bayh-Dole Act of 1980, maintain rights to the intellectual property they produce from federally funded research discoveries. IP theft can therefore result in significant monetary losses for universities as well as risks to America’s national and economic security.

Over the last several years, universities have been actively working to inform their researchers about possible risks associated with contracts and agreements with entities from specific foreign countries, educate them about potentially malign foreign talent programs, and to ensure that they properly disclose to their institution and federal research agencies their relationships and funding received from outside foreign sources. AAU staff along with our 69 U.S.-based member universities and other associations have also been working closely with federal research agencies and intelligence agencies, including the Federal Bureau of Investigation (FBI), to better understand threats posed by foreign actors in order to mitigate risk and address research security concerns on campus.

Indeed, universities are working every day to secure and protect the integrity of the research they conduct on behalf of the federal government from threats posed by malign foreign actors. Actions taken include:

Research Security Strategy and Coordination: Universities have established campus-wide working groups and task forces on research security which regularly meet to review the latest threats and effective practices and discuss policy implementation. Institutions have also established a chief

research security officer position to coordinate and oversee campus efforts to protect and secure research.

Research Faculty Awareness Building Efforts: Universities have created centralized websites and increased direct faculty communications to make sure that they fully understand current federal disclosure requirements related to research security and risks associated with certain international collaborations.

Risk Assessment and Mitigation Review Process: Universities have developed risk criteria and use of comprehensive review processes for review of grants, contracts, and foreign gifts. To this end, some institutions have established new risk management committees for discussion and review of international engagements and collaborations.

Research Security Training Requirements: Now that the National Science Foundation (NSF) has released the completed research security training modules¹ as required by the CHIPs and Science Act of 2022, institutions are incorporating the modules into existing training platforms and requirements. The training modules help provide a baseline understanding of research security concerns across the research enterprise which re. Some institutions are also providing additional training to researchers whose research has been identified as potentially more vulnerable to security breaches or foreign malign influence.

Policies on Disclosure of Conflicts of Interest, Conflicts of Commitment and Foreign Funding

Sources: Universities have reviewed their conflict of interest and conflict of commitment policies and made updates to faculty disclosure policies to more clearly identify foreign affiliations, relationships, and financial interests.

Engagement and Coordination with Federal Intel Agencies and Security Officials: Universities regularly meet and have built strong relationships with their local FBI offices. Universities also engage research funding agencies when they need to mitigate and resolve a research security issue.

Policies on Foreign Gifts and Contracts Reporting: Universities have assessed their policies on reporting foreign gifts and contracts and have improved their reporting procedures as part of Section 117 of the Higher Education Act.

Policies on International Travel: Universities have developed new risk-based international travel policies for faculty and staff, some require researchers to pre-register their foreign travel. Importantly, many institutions offer tailored training briefings to specific faculty before they travel to destinations considered high-risk. For those faculty, universities help mitigate risks by providing secure loaner laptops and encouraging faculty to not cross international borders with devices containing research data.

¹ NSF research security training modules now available, January 30, 2024: <https://new.nsf.gov/news/nsf-research-security-training-modules>

Policies on International Visitors to Campus: Universities have developed requirements for vetting and securely hosting foreign visitors while on campus including centralized processes for evaluating prospective visitors against restricted party lists, U.S. sanction programs, export controls, and other research security topics.

Policies on Export Control Compliance: Universities have comprehensive policies regarding whether and how they will undertake export-controlled research activities. This includes using restricted party screening software within shipping, procurement, and academic visitor processes. Additionally, universities have an export control officer (or officers) with overall responsibility for ensuring university compliance with export control rules and other security controls. On many campuses, faculty training to ensure compliance with export controls requirements is already in place.

Cybersecurity Protocols: Universities have identified appropriate protections for sensitive data in grants and contracts to ensure compliance with NIST SP 800-171. More than 600 institutions are also part of the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) which monitors the threat landscape and shares threat information with its network. Institutions have also taken measures to improve data security and use encryption, multi-factor authentication, and virus scanning tools.

Congress has also enacted several provisions to address research security through the CHIPS and Science Act of 2022 and the National Defense Authorization Act.² Our universities have and will continue to work to ensure compliance with these congressional requirements.

Starting from language in the FY2020 National Defense Authorization Act,³ which mandated the creation of the National Science and Technology Council's (NSTC) interagency subcommittee on research security, NSPM-33 and its implementation guidance specifically called for the effective coordination and harmonization of research security requirements across federal research agencies. This includes the recent finalization of common disclosure elements and forms.⁴

AAU, along with several other higher education associations, research organizations, and universities, also submitted extensive comments⁵ to OSTP's request for information⁶ on the draft research security program guidance.⁷ AAU's comments, similar to several other submitted comments, described significant concerns with the lack of a risk-based approach to research security and the need for clear

² University and Federal Actions Taken to Address Research Security Issues, updated January 4, 2024:

<https://www.aau.edu/key-issues/university-and-federal-actions-taken-address-research-security-issues>

³ Securing American Science and Technology Act (SASTA), Section 1746 of the FY20 NDAA (P.L. 116-92)

⁴ NSTC Research Security Subcommittee, NSPM-33 Implementation Guidance, Disclosure Requirements & Standardization: https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp

⁵ AAU Submits Response to OSTP Request for Information on NSPM-33, May 31, 2023: <https://www.aau.edu/key-issues/aau-submits-response-ostps-request-information-nspm-33>

⁶ Request for Information; NSPM-33 Research Security Programs Standard Requirement, March 7, 2023: <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement>

⁷ Subcommittee on Research Security, National Science and Technology Council, Office of Science and Technology Policy, DRAFT Research Security Programs Standard Requirement, February 2023: https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

and consistent guidance across research agencies when implementing research security program requirements. However, since the June 2023 comment deadline, OSTP has not yet released final requirements or an update to the research community on the status of finalizing the requirements. We are hopeful that by issuing final guidance, OSTP and other federal agencies will take seriously concerns AAU and other associations have raised in the comments to ensure that any final guidance is both risk-based and harmonized across federal agencies. Significant variation in what agencies require for acceptable research security programs will make compliance difficult and would not be in our national interest.

As the threats to the research environment continue to evolve, we look forward to continuing to engage with the committee on issues related to research security and share how America's leading research universities are approaching these issues. Thank you again for holding this important hearing.



Arizona State University
Boston University
Brandeis University
Brown University
California Institute of Technology
Carnegie Mellon University
Case Western Reserve University
Columbia University
Cornell University
Dartmouth College
Duke University
Emory University
The George Washington University
Georgia Institute of Technology
Harvard University
Indiana University
The Johns Hopkins University
Massachusetts Institute of Technology
McGill University
Michigan State University
New York University
Northwestern University
The Ohio State University
The Pennsylvania State University
Princeton University
Purdue University
Rice University
Rutgers University – New Brunswick
Stanford University
Stony Brook University –
State University of New York
Texas A&M University
Tufts University
Tulane University
University at Buffalo –
State University of New York
The University of Arizona
University of California, Berkeley
University of California, Davis
University of California, Irvine
University of California, Los Angeles
University of California, Riverside
University of California, San Diego
University of California, Santa Barbara
University of California, Santa Cruz
The University of Chicago
University of Colorado Boulder
University of Florida
University of Illinois, Urbana-Champaign
The University of Iowa
The University of Kansas
University of Maryland, College Park
University of Miami
University of Michigan
University of Minnesota, Twin Cities
University of Missouri, Columbia
The University of North Carolina at
Chapel Hill
University of Notre Dame
University of Oregon
University of Pennsylvania
University of Pittsburgh
University of Rochester
University of South Florida
University of Southern California
The University of Texas at Austin
University of Toronto
The University of Utah
University of Virginia
University of Washington
The University of Wisconsin – Madison
Vanderbilt University
Washington University in St. Louis
Yale University

February 13, 2024

Dr. Arati Prabhakar
Director
White House Office of Science and Technology Policy
Eisenhower Executive Office Building
1650 Pennsylvania Ave NW
Washington, DC 20502

Dear Director Prabhakar:

Representing America's leading research universities, I write on behalf of the Association of American Universities (AAU) to urge you to consider concerns expressed in the comments from AAU and other associations as you work to finalize the research security program standard requirements which the White House Office of Science and Technology Policy (OSTP) released as a draft for comment in March 2023.

AAU, along with several other higher education associations, research organizations, and universities, submitted extensive comments¹ to OSTP's request for information² on the draft research security program guidance.³ AAU's comments, similar to several other submitted comments, described significant concerns with the lack of a risk-based approach to research security and the need for clear and consistent guidance across research agencies when implementing research security program requirements. We appreciate that consideration of the comments and making appropriate changes to the requirements takes time. Since the June 2023 comment deadline, OSTP has not released final requirements or an update to the research community on the status of finalizing the requirements; we encourage you to finalize the requirements as soon as possible.

Starting from language in the FY2020 National Defense Authorization Act⁴ which mandated the creation of the National Science and Technology Council's (NSTC) interagency subcommittee on research security, NSPM-33 and its implementation guidance specifically called for the effective coordination and harmonization of research security requirements across federal research agencies. At the end of 2023, this coordinated approach led to finalizing common disclosure forms⁵. Building from this success and in continuance of NSPM-33 implementation, we urge OSTP to take seriously concerns AAU and other associations have raised in the comments to ensure that any final guidance is both risk-based and harmonized across federal agencies. Significant variation in what agencies require for acceptable research security programs will make compliance difficult and would not be in our national interest.

¹ AAU Submits Response to OSTP Request for Information on NSPM-33, May 31, 2023: <https://www.aau.edu/key-issues/aau-submits-response-ostps-request-information-nspm-33>

² Request for Information; NSPM-33 Research Security Programs Standard Requirement, March 7, 2023: <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement>

³ Subcommittee on Research Security, National Science and Technology Council, Office of Science and Technology Policy, DRAFT Research Security Programs Standard Requirement, February 2023: https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf

⁴ Securing American Science and Technology Act (SASTA), Section 1746 of the FY20 NDAA (P.L. 116-92)

⁵ NSTC Research Security Subcommittee, NSPM-33 Implementation Guidance, Disclosure Requirements & Standardization: https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp

Finalizing the research security program guidance is critically important for our member institutions. We look forward to continuing to work with OSTP and the interagency subcommittee on research security to refine the requirements and effectively mitigate research security risks related to university-based research.

Sincerely,

A handwritten signature in blue ink that reads "Barbara R. Snyder". The signature is fluid and cursive, with the first name "Barbara" and last name "Snyder" clearly legible.

Barbara R. Snyder
President



United States Government Accountability Office

Report to Congressional Committees

January 2024

RESEARCH SECURITY

Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats

Accessible Version

GAO Highlights

Highlights of [GAO-24-106227](#), a report to congressional committees

Why GAO Did This Study

According to the National Science Foundation, federal agencies obligated about \$1.4 billion for R&D with foreign entities in fiscal year 2020 (the most recent data available). However, some foreign entities may try to exploit U.S. openness in sharing R&D for nefarious purposes.

The Research and Development, Competition, and Innovation Act includes a provision for GAO to review research funding provided to foreign entities of concern. The act's definition of such entities includes foreign terrorist organizations and foreign entities subject to the control, ownership, and jurisdiction of Russia, China, North Korea, and Iran.

This report examines challenges in identifying R&D funds awarded to foreign entities of concern and requirements for awarding and monitoring such funding.

GAO searched USAspending.gov and reviewed documents from federal funding and law enforcement agencies. GAO also interviewed federal agency officials, including those from the five agencies that obligated the most R&D funding in fiscal year 2020.

What GAO Recommends

GAO is recommending that OSTP facilitate information sharing among agencies on identifying foreign ownership, control, or influence. OSTP concurred with this recommendation.

View [GAO-24-106227](#). For more information, contact Candice N. Wright at (202) 512-6888 or wrightc@gao.gov.

January 2024

RESEARCH SECURITY

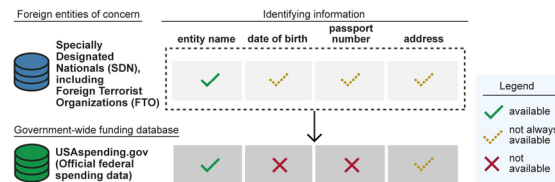
Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats

What GAO Found

GAO found that determining whether federal research and development (R&D) funds were provided to a foreign entity of concern is challenging. Such entities include foreign terrorist organizations and specially designated nationals, among others. Awarding agencies are generally prohibited from doing business with foreign terrorist organizations and specially designated nationals.

GAO found that government-wide databases which report on some of these entities lack common identifying information such as a unique identifier or personally identifiable information. For example, a physical address, date of birth, or other identifying information for entities on the foreign terrorist organization list is often unavailable as entities often try to conceal their identity or location, according to the Treasury Department. When personally identifiable information such as date of birth is available, similar information is not available in the public federal funding data source, USAspending.gov. Specifically, although awarding agencies collect other identifying information, such as phone numbers of entities seeking an award, not all such information is reported in USAspending.gov. Together, these challenges limit the ability to match foreign entities on certain lists with those receiving government-wide funding.

Example of Gaps in Crossmatching Identifying Information for Restricted Foreign Entities With Federal Spending Data



Source: GAO analysis of agency information and publicly available information on U.S. government websites; GAO (icons). | GAO-24-106227

GAO found that some requirements exist specific to R&D awards to foreign entities of concern. For example, agencies are generally required to vet potential awardees against the federal exclusions list, which includes foreign terrorist organizations and specially designated nationals. Agencies that GAO interviewed reported challenges in identifying foreign ownership, control, or influence. Officials from two agencies we reviewed said they use analytical tools and other available information to try to identify foreign ownership. Such efforts, however, are not shared across agencies. Recent guidance from the Office of Science and Technology Policy (OSTP)—the lead federal agency for interagency coordination on science and technology policies—does not address the issue of foreign ownership, control, or influence. OSTP officials told GAO that they handle this issue on a case-by-case basis and acknowledged the challenges that agencies face in addressing such risks. Information sharing on such complex matters would better position agencies to more fully safeguard R&D funds.

United States Government Accountability Office

Contents

GAO Highlights		ii
	Why GAO Did This Study	ii
	What GAO Recommends	ii
	What GAO Found	ii
Letter		1
	Background	5
	Lack of Common Identifying Information Hinders Ability to Identify Research Funds Provided to Foreign Entities of Concern	9
	Some Federal Requirements Exist Specific to Foreign Entities of Concern	17
	Conclusions	30
	Recommendation for Executive Action	31
	Agency Comments	31
Appendix I: Objectives, Scope, and Methodology		34
Appendix II: Research and Development (R&D) Federal Funding Obligated to Entities Located in China and Russia		40
Appendix III: Examples of Information Used by the Department of Defense to Inform Fundamental Research Mitigation Decisions		45
Appendix IV: GAO Contact and Staff Acknowledgments		47
Tables		
	Table 1: Foreign Entities of Concern as Defined by the Research and Development, Competition, and Innovation Act	8
	Table 2: Data Challenges Related to Foreign Entities of Concern as Defined by the Research and Development, Competition, and Innovation Act	12
	Table 3: U.S. Agency-Reported Obligations through Prime Awards to Entities in China ^a and Russia, Fiscal Years 2017-2022	15
	Table 4: Key Government-wide Requirements and Guidance for Research and Development Awards that Involve Foreign Entities of Concern	19
	Table 5: Key Agency-Specific Requirements for Awarding R&D Funding to Foreign Entities of Concern	24

Table 6: Recent Agency-Specific Actions to Mitigate Risk in Awarding Research & Development Funding to Foreign Entities of Concern	26
Table 7: Obligations Funded in Fiscal Years 2017-2022 for Research & Development Awards Made Directly to Entities Located in China ^a and Russia	40
Table 8: Examples of Information Used by the Department of Defense (DOD) to Assess a Covered Individual's Associations, Affiliations, and Collaborations and the Policies of the Proposing Institution that Employs the Covered Individual	45

Figures

Example of Gaps in Crossmatching Identifying Information for Restricted Foreign Entities With Federal Spending Data	ii
Figure 1: Generalized Research and Development Award Process	5
Figure 2: Identifying Information on Foreign Entities of Concern in Government-wide Data Systems	10
Figure 3: Generalized Steps Agencies Take to Address Prohibited or Restricted Foreign Entities	21

Abbreviations

Commerce	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
FTO	Foreign Terrorist Organization
FY	Fiscal Year
GSA	General Services Administration
HHS	Department of Health and Human Services
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorization Act
NIH	National Institutes of Health
NSF	National Science Foundation
NSPM-33	National Security Presidential Memorandum 33
OFAC	Department of the Treasury Office of Foreign Assets Control
OSTP	Office of Science and Technology Policy
R&D	research and development
SAM.gov	System for Award Management
SDN	Specially Designated Nationals and Blocked Persons List
State	Department of State

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

January 11, 2024

Congressional Committees

The United States has long been a global leader in advancing the frontiers of science and technology because of its public and private investments in research and development (R&D)—the creative and systematic work undertaken to increase knowledge and to devise new applications of available knowledge.¹ As the pace of innovation has quickened, competition in the global economy has accelerated. The United States remains at the forefront of scientific and technological discovery and is the world's single largest R&D funder.²

Specifically, federal agencies obligated about \$1.4 billion for R&D awards with foreign entities in fiscal year (FY) 2020.³ We previously reported that federal agencies sometimes provide research funds to foreign entities such as universities, laboratories, and public health organizations.⁴ Agencies may also collaborate with foreign entities to access resources such as talent and expertise, certain environments and populations, and one-of-a-kind scientific facilities. However, some foreign entities may try to exploit U.S. openness in sharing R&D for nefarious purposes. For example, the National Institutes of Health (NIH) became concerned that a researcher at a U.S. university had failed to disclose, among other things, foreign research activity on their grant applications. This led to the researcher's conviction in May 2020 for filing a false tax return that did not

¹National Science Foundation, National Center for Science and Engineering Statistics, *Definitions of Research and Development: An Annotated Compilation of Official Sources*, NCSES 22-209 (Alexandria, VA: May 19, 2022).

²American Association for the Advancement of Science, *Federal R&D Budget Trends: A Short Summary* (Washington, D.C.: Jan. 2019).

³National Science Foundation, National Center for Science and Engineering Statistics, *Federal Funds for Research and Development* (Alexandria, Va.: Apr. 28, 2022). The U.S. obligated about \$167 billion for R&D in FY 2020. R&D awards can include, among other award mechanisms, contracts, grants, and cooperative agreements, which collectively we refer to as "awards." Fiscal year 2020 is the most recent and complete data available.

⁴See GAO, *Federal Research: Information on Funding for U.S.-China Research Collaboration and Other International Activities*, [GAO-22-105313](#) (Washington, D.C.: Sept. 29, 2022). GAO, *Federal Spending: Information on U.S. Funding to Entities Located in China*, [GAO-23-105538](#) (Washington, D.C.: Apr. 12, 2023).

Letter

include his foreign income for his simultaneous employment at two different Chinese universities where he was conducting research.⁵

Congress, the White House, and others have expressed concerns about entities from certain foreign countries, such as China, exploiting U.S. funded research in ways that could harm U.S. national security or economic competitiveness. Recent federal legislation aims to improve the research security environment. The Research and Development, Competition, and Innovation Act was enacted in August 2022 as part of what is commonly referred to as the CHIPS and Science Act of 2022 (the Act).⁶ It includes provisions for federal agencies and federally funded research institutions to address threats to the U.S. research enterprise.

The Act also includes a provision for GAO to examine R&D funding to foreign entities of concern.⁷ This report: (1) describes challenges faced in identifying R&D funds made available to foreign entities of concern and how much funding was provided to foreign entities of concern in FY 2017 through FY 2022 and (2) examines the requirements for awarding and monitoring⁸ of such funding.

The Act defines a "foreign entity of concern" as a foreign entity that is:⁹

- on the Foreign Terrorist Organization (FTO) list;¹⁰
- on the Specially Designated Nationals and Blocked Persons (SDN) list;

⁵Department of Justice press release, *Former Emory University Professor and Chinese "Thousand Talents" Participant Convicted and Sentenced for Filing a False Tax Return* (Washington, D.C.: May, 11, 2020), available at <https://www.justice.gov/opa/pr/former-emory-university-professor-and-chinese-thousand-talents-participant-convicted-and>.

⁶Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, 136 Stat. 1366 (2022).

⁷Pub. L. No. 117-167, div. B, tit. VI, sub. D, §10635, 136 Stat. 1366, 1668-69 (2022).

⁸For the purposes of this report, "monitoring" includes both monitoring and tracking of funds.

⁹Pub. L. No. 117-167, div. B, tit. VI, sub. D, §10638(3), 136 Stat. 1366, 1670 (2022). For the purposes of this report, we also include individuals as "entities."

¹⁰As designated by the Secretary of State under section 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a)).

Letter

- owned by, controlled by, or subject to the jurisdiction or direction of a "covered nation", as defined by 10 U.S.C. § 4872, which are the Democratic People's Republic of North Korea, the People's Republic of China, the Russian Federation, or the Islamic Republic of Iran;
- alleged by the Attorney General to have been involved in activities for which a conviction was obtained under a series of specified federal laws, including the Espionage Act and the Arms Export Control Act;¹¹ or
- engaged in conduct that is detrimental to national security or foreign policy, as determined by the Secretary of Commerce in consultation with the Secretary of Defense and Director of National Intelligence.

To address the first objective, we collected publicly available information on foreign entities included on the FTO and SDN lists from agency websites.¹² The FTO list is comprised of organizations, and the SDN list includes both organizations and individuals. We also collected information from the Department of Justice (DOJ) on foreign entities—individuals and organizations—convicted under the statutory provisions identified in the Act. We then searched USAspending.gov to identify whether any R&D funds were provided to these entities.¹³ Specifically, we searched for matches—in the names and addresses of entities on the lists (such as the SDN list)—with similar information in USAspending.gov to determine

¹¹The full list of laws specified in the definition of foreign entity of concern are: 18 U.S.C. ch. 37, (commonly known as the Espionage Act); 18 U.S.C. §§ 951, 1030; 18 U.S.C. ch. 90, (commonly known as the Economic Espionage Act of 1996); the Arms Export Control Act (22 U.S.C. § 2751 et seq.); sections 224-227, or 236 or the Atomic Energy Act of 1954 (42 U.S.C. §§ 2274 - 2277, 2284); the Export Control Reform Act of 2018 (50 U.S.C. § 4801 et seq.); and the International Emergency Economic Powers Act (50 U.S.C. § 1701 et seq.).

¹²In this report, we collected information on foreign entities reported on the FTO list from the Department of State's website, <https://www.state.gov/foreign-terrorist-organizations/> and information on the SDN list from Treasury's website, <https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>.

¹³The USAspending.gov website is the official public source of government spending data. Agencies are required to report certain information about federal awards that equal or exceed the micro-purchase threshold that are then made available on a single public-facing, searchable website. Federal Funding Accountability and Transparency Act of 2006, Pub. L. No. 109-282, 120 Stat. 1186 as amended by The Digital Accountability and Transparency Act of 2014, Pub. L. No. 113-101, 128 Stat. 1146 (codified as amended at 31 U.S.C. § 6101 note); 2 C.F.R. pt. 170, FAR subparts 4.6 and 4.14.

Letter

whether any foreign entity of concern received R&D funds from FY 2017 through FY 2022.

We also met with relevant agency officials who collect and manage this information and discussed challenges in the availability and reliability of data. Due to the difficulty in determining whether foreign entities are owned by, controlled by, or subject to the jurisdiction of covered nations (China, Iran, North Korea, and Russia), to address funding to these entities we analyzed publicly available country-level obligations data reported by agencies in USAspending.gov.¹⁴ Specifically, we focused on prime awards (grants, cooperative agreements, and contracts) made directly to an entity located in a covered nation in FY 2017 through FY 2022.¹⁵ We requested that agency officials validate the accuracy of prime award data from USAspending.gov, and we refined the data. We found that the prime award data were sufficiently reliable for the purposes of this report.

To address the second objective, we focused on the five agencies that—according to a report by the National Science Foundation (NSF)—obligated the largest amount of R&D funding in FY 2020, the most recent data available when we initiated this review. The five agencies are the NSF; the National Aeronautics and Space Administration (NASA); and the Departments of Defense (DOD), Energy (DOE), and primarily the NIH within Health and Human Services (HHS). We collected agency policies and other documents and interviewed agency officials on requirements for awarding and monitoring federal funds to foreign entities of concern.

We also interviewed officials at the General Services Administration (GSA) about the System for Award Management (SAM.gov), which includes information on entities doing business with the federal government, and at the Office of Science and Technology Policy (OSTP) on its role in providing guidance to federal agencies that fund R&D and

¹⁴An obligation is a definite commitment that creates a legal liability of the government for the payment of goods and services ordered or received, or a legal duty on the part of the United States that could mature into a legal liability by virtue of actions on the part of the other party, beyond the control of the United States. Payment may be made immediately or in the future.

¹⁵For the purposes of this report, we define a prime award as a grant, cooperative agreement, or contract awarded by the U.S. government directly to a non-federal entity for the purpose of carrying out a federal program.

Letter

the institutions that perform the work. For more information on the objectives, scope, and methodology, see appendix I.

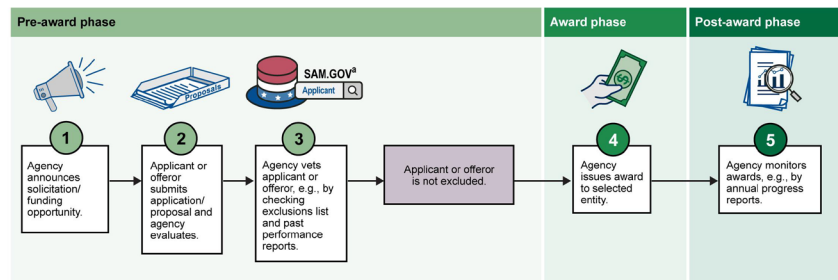
We conducted this performance audit from August 2022 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal Process for Determining Eligibility to Receive Funds

Federal agencies generally follow a phased process for providing R&D funds to an award recipient (fig. 1).

Figure 1: Generalized Research and Development Award Process



Source: GAO analysis of agency information, regulations, and guidance; GAO (icons). | GAO-24-106227

*The System for Award Management (SAM.gov) is a U.S. government website that includes entity registrations for those entities that would like to do business with the government, including those entities seeking to apply for federal grants or loans or propose on a federal contract. Among other things, SAM.gov also contains data on excluded entities. According to agency officials, they can also vet applicants using agency-specific or other internal government data sources to determine

Letter

suitability. In such internal sources, other identifiable information may be available on the applicant or offeror.

In general, there are three phases:

- The pre-award phase begins with an agency announcing a funding opportunity or solicitation. For prime awards—including contracts, grants, and cooperative agreements—an applicant or offeror submits an application or proposal.¹⁶ As part of the application or proposal evaluation process, the awarding agency evaluates information about and provided by the applicant or offeror to ensure it is qualified to conduct the research.¹⁷
- In the award phase, the awarding agency issues the award to the entity selected for work and begins to obligate funds.
- In the post-award phase, the awarding agency monitors the awardee to ensure compliance with the award terms. This process occurs throughout the period of performance of the award and includes the review of progress or other reports submitted by the awardee. At the end of the period of performance, the awarding agency reviews the final financial and progress or technical reports to close out the award.

Federal agencies report information on R&D funds made through prime awards, which is, in turn, made available to the public in USAspending.gov in accordance with the requirements outlined in the Federal Funding Accountability and Transparency Act (FFATA) of 2006, as amended, and implementing regulations and guidance.¹⁸

¹⁶For the purposes of this report, we use the term “applicant” to include offerors and applicants responding to solicitations or funding announcements posted by federal agencies for prime awards.

¹⁷For some agencies, the evaluation phase can include a required peer review process.

¹⁸Pub L. No. 109-282, 120 Stat. 1186 as amended by The Digital Accountability and Transparency Act of 2014, Pub. L. No. 113-101, 128 Stat. 1146 (codified as amended at 31 U.S.C. § 6101 note); 2 C.F.R. pt. 170, FAR subparts 4.6 and 4.14.

Letter

Some Entities are Excluded from Receiving Federal Funding

Entities seeking prime awards are generally required to register in SAM.gov, which is managed by GSA.¹⁹ Some entities are excluded from receiving federal contracts, certain subcontracts, and types of federal financial and nonfinancial assistance and benefits. An active exclusion means an entity is currently debarred, suspended, proposed for debarment, or declared ineligible for these awards. These entities are included in the SAM.gov exclusions data. The exclusions list also includes entities that are designated with prohibition/restriction where the scope of the exclusion from receiving federal funds is determined by the specific program or law under which the entity has been prohibited or restricted. Entities on the FTO and SDN lists are included on the SAM.gov exclusions list and denoted as "prohibition/restriction." Awarding agencies are generally required to check the SAM.gov exclusions list prior to making an award.²⁰

Foreign Entities of Concern

The key elements of the definition of "foreign entity of concern" include long-established sanctions lists, four covered nations, and entities related to convictions obtained under specified U.S. laws. Table 1 provides information on the key elements included in the definition of "foreign entity of concern."

¹⁹Individuals who apply as a natural person for federal financial assistance, including grants and cooperative agreements, are not required to register in SAM.gov. 2 C.F.R. § 25.110(b). See 2 C.F.R. § 25.110 and FAR 4.1102 for exceptions to SAM.gov registration requirements for those seeking federal financial assistance, including grants and cooperative agreements and contracts respectively.

²⁰For grants and cooperative agreements, 2 C.F.R. § 180.430 directs agency officials to check SAM.gov exclusions before entering into covered transactions. However, not all transactions are covered transactions. For example, direct awards to foreign governments and foreign government entities are generally not covered transactions; therefore, agencies are not required to check SAM.gov exclusions for such transactions (2 C.F.R. § 180.215). Regardless, agency officials are prohibited from entering into any transaction with a disqualified entity if the entity is disqualified for that transaction according to 2 C.F.R. § 180.400. To identify a disqualified entity, an agency would need to check SAM.gov exclusions before providing federal funds. Most of the agencies we reviewed told us they check SAM.gov regardless of these exemptions.

Letter

Table 1: Foreign Entities of Concern as Defined by the Research and Development, Competition, and Innovation Act

Definition from Act	Description from Federal Laws, Regulations, and Agency Information
Foreign Terrorist Organizations (FTO)	Foreign Terrorist Organizations (FTOs) are foreign organizations that are designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended. It is unlawful for a person in the United States or subject to its jurisdiction to knowingly provide a designated FTO with "material support or resources" including tangible or intangible property, or services, including currency or monetary instruments, and expert advice or assistance, which is advice or assistance derived from scientific, technical, or other specialized knowledge. The organizations' names are publicly listed on the State Department website and updated when a new designation is made by the Secretary of State.
Specially Designated Nationals and Blocked Persons (SDN)	The Department of the Treasury's Office of Foreign Assets Control, as part of its enforcement efforts, publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities—such as terrorists and narcotics traffickers—designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and people in the United States are generally prohibited from dealing with them. This list is searchable or downloadable from the Treasury website and is updated by the Department as frequently as multiple times per week.
Entities owned by, controlled by, or subject to the jurisdiction or direction of a government of a foreign country that is a covered nation (as such term is defined in section 4872 of title 10, United States Code)	10 U.S.C. § 4872 defines "covered nations" as the Democratic People's Republic of North Korea, the People's Republic of China, the Russian Federation, and the Islamic Republic of Iran.
Entities alleged by the Attorney General to have been involved in activities for which a conviction was obtained under the federal laws cited in section 10638(3)(D) of the Research and Development, Competition, and Innovation Act	Section 10638(3)(D) listed the following laws: • 18 U.S.C. ch. 37, commonly known as the Espionage Act; • 18 U.S.C. §§ 951, 1030; • 18 U.S.C. ch. 90, commonly known as the Economic Espionage Act of 1996; • the Arms Export Control Act, 22 U.S.C. § 2751 et seq.; sections 224-227, or 236 of the Atomic Energy Act of 1954; 42 U.S.C. §§ 2274-2277, 2284; • the Export Control Reform Act of 2018, 50 U.S.C. § 4801 et seq.; and • the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq.
Entities determined by the Secretary of Commerce, in consultation with the Secretary of Defense and the Director of National Intelligence, to be engaged in unauthorized conduct that is detrimental to the national security or foreign policy of the United States	The phrase also appeared in the definition of "foreign entity of concern" found in the Creating Helpful Incentives to Produce Semi-Conductors for America Act, found in the National Defense Authorization Act for Fiscal Year 2021. That law prohibits the Secretary of Commerce from providing financial incentives for semiconductor development to "foreign entities of concern."

Source: GAO analysis of federal laws, regulations, and agency information. | GAO-24-106227

Letter

Lack of Common Identifying Information Hinders Ability to Identify Research Funds Provided to Foreign Entities of Concern

We found that, due to a lack of common identifying information (such as a unique identifier or personally identifiable information) on foreign entities of concern in federal government databases, determining whether federal funds were provided to such entities is challenging. For example, common identifying information for the entities on the foreign terrorist organization list is not publicly available. We were able to identify some information on R&D funding provided to entities in China and Russia.

Common Identifying Information across Data Sources is not Always Available

Identifying information for foreign entities of concern—such as a unique identifier, physical address, an individual's date of birth, or passport number—is not fully available across federal data sources. This is primarily due to the nature of the entities themselves, who may try to hide their location or identity, according to Treasury officials. For example, for some foreign terrorist groups as well as some individuals on the SDN list, address, date of birth, or passport information is not available. In addition, while most of the entity lists include individuals, awards are generally made to organizations, research institutions, or businesses rather than individuals, according to agency officials. Furthermore, USAspending.gov—the government-wide federal funding data source—does not include certain personally identifiable information (including for foreign entities) due to existing privacy laws and regulations.²¹ According to USAspending.gov, due to existing laws and regulations, some data such as date of birth or passport are not captured. Awarding agencies collect identifying information such as name, address, email, phone,

²¹The USAspending.gov "Data Sources" document states that due to existing laws and regulations, some data—including personally identifiable information—are not published. <https://www.usaspending.gov/data/about-the-data-download.pdf>. The SAM.gov website is the official source for information on entities, including those that are prohibited or restricted, among other things. SAM.gov data on registrants links to USAspending.gov award recipients' data via the SAM.gov unique entity ID (UEI)—the primary method to identify entities throughout the federal awarding life cycle and in other federal systems. The SAM.gov website does not publicly display "sensitive" information on individuals in the exclusions list, such as their street address, but such information, to the extent available, may be accessed by authorized U.S. government users.

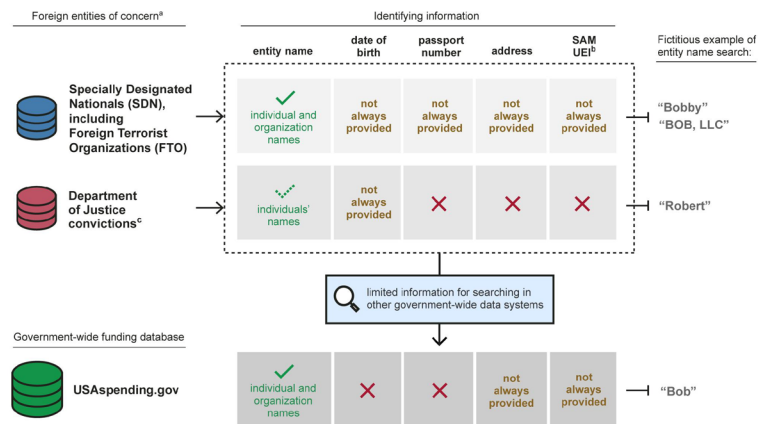
Letter

employment, and previous award history from entities seeking a research award, but not all this information is reported in government-wide data sources.

These challenges limit the ability to match foreign entities on certain lists and those receiving government-wide funding as reported in USAspending.gov.

Figure 2 shows identifying information available for foreign entities of concern that are contained in federal data systems used to vet entities and report on federal funds.²²

Figure 2: Identifying Information on Foreign Entities of Concern in Government-wide Data Systems



Source: GAO analysis of agency information and publicly available information on U.S. government websites; GAO (icons). | GAO-24-106227

²²For the purposes of this report, we use the term "vet" to refer to a process by which agencies gather information on the potential awardees to verify their suitability for an award. DOD told us they use the term "due diligence" to describe such efforts, and that for DOD the term "to vet" refers to either target development or personnel vetting for employment.

Letter

"Foreign Entity of Concern" is defined by the Research and Development, Competition, and Innovation Act as a foreign entity (1) on the Foreign Terrorist Organization (FTO) list; (2) on the Specially Designated Nationals and Blocked Persons (SDN) list; (3) under the ownership, control, or jurisdiction or direction of China, Iran, North Korea, or Russia; (4) alleged by the Attorney General to have been involved in activities for which a conviction was obtained by the Department of Justice (DOJ) under specified laws, including the Espionage Act and the Arms Export Control Act; or (5) determined by the Secretary of Commerce in coordination with the Secretary of Defense and the Director of National Intelligence to be engaged in unauthorized conduct that is detrimental to U.S. national security or foreign policy.

^bSAM unique entity ID (UEI) is the primary key to identify entities throughout the federal awarding life cycle, in SAM.gov, and in other federal systems.

^cAccording to DOJ officials, the agency does not compile data on entities allegedly involved in activities for which there was a conviction by DOJ under the specified statutory provisions and such a list is not publicly available. DOJ provided information on entities convicted under the laws specified in the definition of foreign entity of concern in the Act.

Example of a Hypothetical Business Name Search in USAspending.gov

A search in USAspending.gov for "Contractor Night"—a contractor which manages and operates an agency-funded national laboratory located in Fictional, Texas—showed the same entity listed under four name variations in the system: "Night," "Contract Night," "Night Contractor," and "Night Limited Liability Company." A search for "Contract Night" in USAspending.gov also shows results for "Contractor Night and Day." However, the address information in USAspending.gov for "Contractor Night and Day" is Day, Florida, and not Fictional, Texas, indicating it may not be the same entity as "Contract Night."

Source: Anonymized example based on actual GAO experience in conducting a name search in USAspending.gov | GAO-24-106227

Specifically, we found that name variations for entities differ across and even within the various data systems when attempting to crossmatch names across systems. As represented in figure 2 above, a fictitious entity called "BOB, LLC" included on the list of foreign terrorist organizations may or may not be related to an individual named "Bob" listed in another data system. (See sidebar for an illustrative example of a name search in USAspending.gov). A name match alone does not provide sufficient or reliable information to conduct matches with awardees in USAspending.gov. Additional identifying information—such as an address—is needed to identify the entity with some assurance. USAspending.gov publishes information on addresses, but we have

Letter

previously reported that USAspending.gov data are not always complete or accurate.²³

According to agency officials, they can also vet applicants using agency-specific or other internal government data sources to determine suitability. In such internal sources, other identifying information collected through the application or proposal documents may be available on the applicant. For example, the application or proposal may include identifying information such as an address.

Table 2 highlights key data challenges across the different sources of information on foreign entities of concern.

Table 2: Data Challenges Related to Foreign Entities of Concern as Defined by the Research and Development, Competition, and Innovation Act

List and Lead Agency ^a	Challenges Related to Available Data or Lack Thereof
Foreign Terrorist Organizations (FTO) Department of State	The State website provides information on names of Foreign Terrorist Organizations only. Due to limited available information—name only—making a definitive match with a federal funding data source is challenging.
Specially Designated Nationals and Blocked Persons (SDN) Department of the Treasury	The Treasury website provides information on named entities—such as an address, date of birth, alias, country of residence, or passport number—to the extent such information is available and can be verified. The SDN list includes FTOs and some individuals who may be associated with them. For some of these entities, minimal identifying information is available (i.e., names and address or country). In addition, some have multiple (in some cases dozens) of “also known as” (AKAs) or name spelling variations. In part, these variations result from translating names from other alphabets (e.g., Cyrillic or Arabic) to English. Due to a lack of consistent information across all entities included in the SDN list, making a definitive match with a federal funding data source is challenging.

²³We have previously reported on issues with the completeness, accuracy, and quality of USAspending.gov data and have identified opportunities for improvement. GAO, *Federal Spending Transparency: Opportunities Exist to Further Improve the Information Available on USAspending.gov*, [GAO-22-104702](#) (Washington, D.C.: Nov. 8, 2021); *Data Act: Quality of Data Submissions Has Improved but Further Action Is Needed to Disclose Known Data Limitations*, [GAO-20-75](#) (Washington, D.C.: Nov. 8, 2019); and *DATA Act: OMB, Treasury, and Agencies Need to Improve Completeness and Accuracy of Spending Data and Disclose Limitations*, [GAO-18-138](#) (Washington, D.C.: Nov. 8, 2017). We have also reported on data quality issues that agencies’ inspectors general have identified—see GAO, *Federal Spending Transparency: OIGs Identified a Variety of Issues with the Quality of Agencies’ Data Submissions*, [GAO-22-105427](#) (Washington, D.C.: July 12, 2022). Of the 17 recommendations GAO made in these reports, 10 have been implemented as of November 2023. We will continue to follow up with the agencies on their implementation of the remaining seven recommendations.

Letter

List and Lead Agency ^a	Challenges Related to Available Data or Lack Thereof
Entities allegedly involved in activities for which a conviction was obtained under the laws cited in the Research and Development, Competition, and Innovation Act section 10638(3)(D) Department of Justice (DOJ)	The Executive Office for United States Attorneys (EOUSA) in DOJ maintains a case management system, CaseView, to track certain case-related data fields, including names and other pertinent case information for individuals and organizations convicted of a federal crime. However, CaseView does not specifically track or allow for the identification of "foreign entities of concern." Further, EOUSA is not aware of any other such list maintained by DOJ. Officials told us that gathering this information would require an in-depth analysis of the specific facts for each individual or organization involved in certain identified cases. Since these specific data are not maintained or readily available, we collected data from EOUSA related to convictions under the laws specified in the Act during our time frame (FY 2017 - FY 2022). Most of the convictions involved individuals, and for some of the conviction data, EOUSA was able to include a date of birth or country of citizenship, but not all. Officials noted, however, that personally identifiable information maintained in CaseView—such as date of birth, country of citizenship, and address information—may not be reliable because these data are provided by an investigative agency at the beginning of an investigation when such information may be unverified. Due to these issues, making a definitive match with a federal funding data source is challenging.
Entities under "covered nations" Federal Awarding Agencies	R&D funding agencies we reviewed do not have a list of entities "owned by, controlled by, or subject to the jurisdiction or direction" of North Korea, China, Russia, or Iran. These agencies told us they often lack reliable data and information on R&D awardees' foreign ownership, control, or influence. In addition, Department of Commerce officials told us that this portion of the definition of foreign entities of concern is new and applies to a limited number of federal agency programs. Due to a lack of information on foreign ownership, jurisdiction, or control for entities, making a definitive match with a federal funding data source is challenging.
Entities determined by Commerce in consultation with the Secretary of Defense and the Director of National Intelligence to be engaged in unauthorized conduct detrimental to U.S. national security or foreign policy Department of Commerce	In September 2023, Commerce issued a final rule implementing conditions in its semiconductor incentives program contained in the CHIPS and Science Act of 2022, which includes a definition of foreign entity of concern. Commerce officials told us that this definition only applies to this Commerce program and does not apply broadly across other federal programs. As part of this final rule, Commerce's definition of foreign entity of concern for its program includes, among other things, foreign entities (1) included on the Bureau of Industry and Security's Entity List (15 CFR part 744, supplement no. 4); (2) included on Treasury's list of Non-SDN Chinese Military-Industrial Complex Companies (NS-CMIC List), or for which one or more individuals or entities included on the NS-CMIC list, individually or in the aggregate, directly or indirectly, hold at least 50 percent of the outstanding voting interest; or (3) determined by the Secretary of Commerce, in consultation with the Secretary of Defense and the Director of National Intelligence, to be engaged in unauthorized conduct that is detrimental to the national security or foreign policy of the United States.^b Due to the timing of this final rule issuance, we were unable to include entities defined by the rule above in the analysis of this engagement.

Source: GAO analysis of agency information. | GAO-24-106227

^aSee table 1 in this report for the full definition of foreign entity of concern from section 10638 of the Research and Development, Competition, and Innovation Act.

^bPreventing the Improper Use of CHIPS Act Funding, 88 Fed. Reg. 65600-65619 (September 25, 2023) (to be codified in 15 C.F.R. pt. 231). The effective date for this rule was November 24, 2023. This rule does not include a specific list of entities determined to be engaged in unauthorized conduct detrimental to U.S. national security or foreign policy.

For R&D awards made between FY 2017 and FY 2022, we found no matches between names of entities on the FTO list and awardees in

Letter

USAspending.gov. In the same time frame, for entities on the SDN list that had a name match with USAspending.gov recipients, address information did not match. Similarly, for entities on the DOJ convictions list for which there was a name match in USAspending.gov, the address information did not match.²⁴

The lack of common identifying information and the nature of the foreign entities of concern themselves limit definitive determinations on whether such entities received federal R&D funding.

²⁴For reporting purposes, to determine with sufficient confidence whether a foreign entity received federal R&D funds, we searched for a match in the entity name and publicly available address information between the list and USAspending.gov. See appendix I for more information on this methodology.

Letter

Some Information on R&D Funding Provided to Entities in China and Russia Is Available

Based on our review of USAspending.gov, we identified funds provided directly to entities located in two of the four covered nations (China and Russia) in FY 2017 through FY 2022 (see table 3 below).²⁵ Specifically, U.S. agencies reported obligating \$26 million through prime awards for R&D to entities in China and \$1.5 million to entities in Russia during this period. Based on our review of USAspending.gov, we did not identify prime awards to entities located in the remaining covered nations—Iran and North Korea—during this period.²⁶

Table 3: U.S. Agency-Reported Obligations through Prime Awards to Entities in China^a and Russia, Fiscal Years 2017-2022

Recipient location country	Awarding agency	Obligations in fiscal years 2017-2022 (in thousands of dollars)			
		Cooperative Agreement	Grant	Contract	Total
China	Centers for Disease Control and Prevention	14,135			14,135
	National Institutes of Health	300	9,415	439	10,154
	Department of Agriculture	1,255	64		1,319
	Department of Defense		175		175
	Department of the Interior		70		70
	HHS Office of the Assistant Secretary for Health		50		50
	CHINA SUBTOTAL				25,904
Russia	Department of Agriculture	563			563
	Department of Commerce			343	343

²⁵These data are publicly available on USAspending.gov and provides information on foreign entities—individuals and organizations—based on the country in which they reside or are located, respectively. See appendix II for further information on these data. We have previously found issues with the completeness, accuracy, and quality of USAspending.gov data—see [GAO-22-104702](#) and [GAO-20-75](#). We have also reported on data quality issues that agencies' inspectors general have identified—see GAO, *Federal Spending Transparency: OIGs Identified a Variety of Issues with the Quality of Agencies' Data Submissions*, [GAO-22-105427](#) (Washington, D.C.: July 12, 2022).

²⁶Some of the award recipients we identified are under the jurisdiction or direction of the governments of China and Russia. For example, direct funds were provided to the Chinese Center for Disease Control and Prevention and the Russian Ministry of Natural Resources and Environment (Yakut Administration for Hydrometeorology and Environmental Monitoring). See app. II for further details on the award recipients identified for this period. We did not verify ownership or control for all the recipients we identified due to challenges with determining foreign ownership discussed later in this report.

Letter

Recipient location country	Awarding agency	Obligations in fiscal years 2017-2022 (in thousands of dollars)			
		Cooperative Agreement	Grant	Contract	Total
	Department of the Interior	12	312		324
	Department of Defense			302	302
	RUSSIA SUBTOTAL				1,531

Source: GAO analysis of USAspending.gov data. | GAO-24-106227

Note: Amounts shown may not sum to totals because of rounding. We analyzed prime award information by awarding agency and calculated the total amount obligated based on the federal action obligation data element. This data element represents the obligation amount agencies reported for award transactions during the period specified. We downloaded award data for fiscal years 2017 through 2022 from USAspending.gov on September 8, 2023.

*We included entities in Hong Kong, a Special Administrative Region of China, in the scope of our review due to the recent change in the treatment of the region by the U.S. government. In July 2020 the President determined in Executive Order 13936 that Hong Kong was no longer sufficiently autonomous to justify differential treatment in relation to China. Specifically, the President suspended the application of section 201(a) of the United States-Hong Kong Policy Act of 1992 to several specified statutes.

As shown in table 3, the CDC obligated the most R&D funding to entities in China, primarily for influenza research. See appendix II for more detailed information on the R&D awards we identified to entities in Russia and China from FY 2017 through FY 2022.

Based on our review, we found one contract where an agency misreported funds as R&D. Specifically, NASA incorrectly recorded \$710 million in obligations as "space research and technology" made from FY 2017 through FY 2022 under a long-standing contract to the Russia Space Agency in support of the International Space Station. However, officials noted that activities under the multi-phased contract had transitioned to primarily "space transportation" (i.e., launch, landing, sustaining engineering, and logistics). NASA officials acknowledged the error, attributing it to overlooking the need to update the information in the Federal Procurement Data System following the transition, and plan to correct the error in response to our observation.²⁷

²⁷The Federal Procurement Data System is the government-wide system for agencies to report information on federally funded contracts. These data are reflected in USAspending.gov.

Letter

Some Federal Requirements Exist Specific to Foreign Entities of Concern

Based on our review of documents and interviews with R&D funding agencies, we found some government-wide requirements exist related to awarding R&D funds specific to foreign entities of concern. For example, some requirements prohibit funding to certain foreign entities of concern. All federal R&D awards have monitoring requirements, but none are specific to awards involving foreign entities of concern. Officials from nearly all the agencies we reviewed noted additional agency specific requirements to address potential risks posed by foreign entities of concern. However, officials reported that agencies face challenges with identifying and addressing risks associated with foreign ownership, control, or jurisdiction. While OSTP has provided guidance to agencies on research security risks, it does not address issues of foreign ownership, control, or influence; agencies told us this is a challenge in vetting applicants.

Government-wide Requirements for Awarding and Monitoring R&D Awards Exist

Government-wide requirements for awarding R&D awards specific to foreign entities of concern include both established and newer requirements. For example, agencies are generally required to vet potential award recipients against the SAM.gov exclusions. These exclusions include entities on the FTO and SDN lists that were established decades ago.²⁸ More recently, OSTP issued government-wide guidance limiting science and technology cooperation with Russian government-affiliated research institutions. In addition, a recent statutory restriction prohibits procurement of telecommunications and surveillance services and equipment from certain Chinese telecommunications

²⁸Some officials stated they also check SAM.gov exclusion information to determine whether a principal investigator/project director and the principal business official included in proposals is excluded. As discussed earlier in this report, the SAM.gov exclusion information includes, among others, entities that are designated with "prohibition/restriction" where the scope of the exclusion from receiving federal funds is determined by the specific program or law under which the entity has been prohibited or restricted. Entities on the FTO and SDN lists are among those included in the SAM.gov exclusions list and identified as "prohibition/restriction."

Letter

companies. Table 4 details key government requirements and guidance for R&D awards that involve foreign entities of concern.

Letter

Table 4: Key Government-wide Requirements and Guidance for Research and Development Awards that Involve Foreign Entities of Concern

Grants and contracts	System for Award Management (SAM.gov) Exclusions List. Federal agencies are generally required to check the exclusions list on SAM.gov—a government-wide website—for potential restrictions or exclusions prior to awarding grants and contracts. The exclusions list includes some entities defined as a foreign entity of concern, such as those entities on the Foreign Terrorist Organizations (FTO) and Specially Designated Nationals and Blocked Persons (SDN) lists. (See 2 C.F.R. §§ 180.425, 180.430, 200.206; FAR § 9.405(e).) Federal guidance and regulations generally prohibit or restrict federal agencies from awarding grants and contracts to parties included on the exclusions list in accordance with the scope of the exclusion or restriction (2. CFR § 180.400, FAR 9.405(a)-(c)).^a 41 U.S.C. § 2313 — Agencies are generally required to review information that is contained in the SAM.gov Responsibility/Qualifications data. Agencies review information which, among other things, should indicate if a prospective contractor was on certain lists maintained by Treasury's Office of Foreign Assets Control (OFAC), including the SDN list or persons sanctioned under the Iran Sanctions Act of 1996 that do not appear on the SDN list.^b Foreign Terrorist Organizations. It is unlawful for a person in the United States to knowingly provide "material support or resources," such as funding or expert scientific or technical training, to a designated FTO. Entities on the FTO list are included in the definition of foreign entities of concern. According to State and OFAC, these prohibitions also apply to federal agencies. Specially Designated Nationals and Blocked Persons. SDN assets are blocked, and U.S. persons are generally prohibited from dealing with them. According to OFAC, these prohibitions also apply to federal agencies. Chinese Telecommunication Equipment Prohibition. Agencies and award recipients are prohibited from procuring or obtaining certain telecommunications and video surveillance services and equipment that are produced by specified Chinese telecommunications companies. (See 2 C.F.R. § 200.216 for award recipients and FAR subpart 4.21 for agency and awardees.) Russia. In June 2022, the Office of Science and Technology Policy issued guidance stating that the federal government was limiting its bilateral science and technology research cooperation with all Russian government-affiliated research institutions (including various international projects and initiatives), except where required by obligations under international law.
Contracts only	Prohibited Sources. FAR subpart 25.7 addresses foreign acquisition prohibited sources and includes prohibitions of most awards to entities included on sanctions lists administered by OFAC, including the SDN list, and most transactions involving Iran.^c This subpart also generally prohibits an agency from entering into a contract for the procurement of goods or services with a person that exports certain sensitive technology to Iran (FAR subpart 25.703-3). Certification Regarding Responsibility. For awards above the simplified acquisition threshold, prospective contractors must certify that, among other things, they are not currently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any federal agency (FAR §§ 9.104, 52.209-5). Contractors are required to certify prior to receiving federal research and development funding.

Source: GAO analysis of agency information, federal laws and regulations. | GAO-24-106227

Note: This table shows government-wide requirements and guidance based on our review of agency documents and interviews. This is not a comprehensive list of all government-wide requirements and guidance which may involve such entities.

^aIssued by the Office of Management and Budget, 2 C.F.R. subtitle A, which includes 2 C.F.R. parts 25, 180, and 200, contains guidance to federal agencies on government-wide policies and procedures for the award and administration of grants and agreements. Federal awarding agencies implement this guidance through agency regulations published in 2 C.F.R. subtitle B and/or in policy and procedural issuances, such as internal instructions.

^bRequirements in 41 U.S.C. § 2313 apply to any person awarded a federal agency contract or grant in excess of \$500,000 and any person awarded such other category or categories of federal agency contract as the FAR may provide, if any of the information included in section 2313(c) exists with

Letter

respect to the person. Information in section 2313(c) includes if the entity is on the SDN list and the list of persons sanctioned under the Iran Sanctions Act of 1996 that do not appear on the SDN list (commonly known as the Non-SDN Iranian Sanctions Act list), 41 U.S.C. §§ 2313(b) and (c)(8). While the FAR and part 2 of the CFR refer to the Federal Awardee Performance Integrity and Performance Information System (FAPIS) as the repository for this information, according to officials in the General Services Administration FAPIS was decommissioned in 2022 with this information moving to SAM.gov at that time; however, the regulations and guidance have not yet been updated to reflect this change.

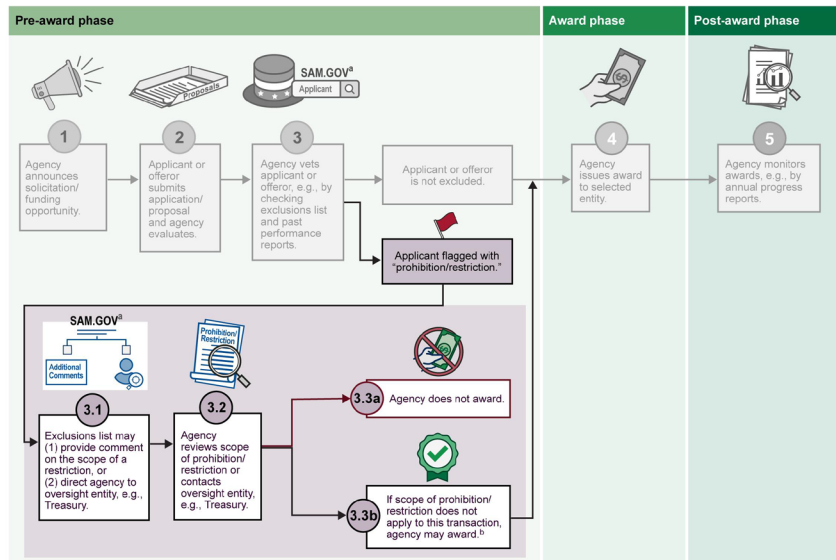
²⁹While part 2 of the C.F.R. does not include a similar specific section addressing prohibited sources, these prohibitions may also apply to grants and cooperative agreements.

Based on our review, we also found that federal award requirements are generally the same for all entities regardless of whether the entity is domestic or foreign.²⁹ For example, as illustrated by figure 3, agencies follow the same process when an entity, domestic or foreign, appears on the SAM.gov exclusions list and is prohibited or restricted from receiving federal funds due to being designated with a “prohibition/restriction” flag. Entities designated with prohibition/restriction include entities on various sanctions lists administered by OFAC, including the SDN list. The scope of the prohibition or restriction on receiving federal funds is determined in accordance with the specific program or law under which the entity is prohibited or restricted.

²⁹While most government-wide requirements do not distinguish between domestic and foreign entities, 2 C.F.R. §200.101(2) states that federal awarding agencies may apply subparts A through E of 2 C.F.R. part 200 to foreign public entities and foreign organizations except where the agency determines that such application would be inconsistent with international responsibilities of the United States or the statutes or regulations of a foreign government. Most agencies told us that they apply 2 C.F.R. part 200 to foreign entities.

Letter

Figure 3: Generalized Steps Agencies Take to Address Prohibited or Restricted Foreign Entities



Source: GAO analysis of agency information, regulations and guidance; GAO (icons). | GAO-24-106227

^aThe System for Award Management (SAM.gov) is a U.S. government website that includes entity registrations for those entities that would like to do business with the government, including those entities seeking to apply for federal grants or loans or propose on a federal contract. Among other things, SAM.gov also contains data on entities prohibited or restricted from receiving federal funds. According to some agency officials, they can also vet applicants using agency-specific or other internal government data sources to determine suitability. In such internal sources, other identifiable information may be available on the applicant.

^bUnder certain circumstances, an agency may also seek a license to provide federal funds to an entity subject to Treasury's Office of Foreign Assets Control sanctions that would otherwise be prohibited.

Letter

For each entity that is flagged as prohibition/restriction in SAM.gov, the information will either (1) provide the scope of the prohibition/restriction or (2) refer the awarding official to the oversight entity for the exclusion. According to OFAC officials, OFAC is responsible for ensuring that any changes (i.e., addition of new or deletion of existing entities) to entities on the SDN list, among other sanctions lists, that result in a restriction or prohibition from receiving federal funds are reflected in the exclusions list. Agency officials use exclusions information in SAM.gov in determining whether an entity is prohibited from receiving federal funds for the proposed award.³⁰

All federal R&D awards have monitoring requirements—often annual reporting requirements—but none are specific to awards to foreign entities of concern. For example, recipients of grant funding are required to submit progress reports and track financial records. For contracts, awardees are required to provide scientific and technical reports and any other information required by reporting requirements in the contract work statement. These reports may include information such as research data, changes to work, plans for budgets, and accomplishments. For contracts, awardees are required to annually submit representations and certifications including ownership or control of the entity, which could alert an agency if an awardee becomes owned by a foreign entity of concern. While there are no government-wide monitoring requirements specific to foreign entities of concern, agencies may choose to enhance their monitoring efforts by, for example, conducting additional site visits or adding requirements for awardees to report more frequently.³¹ Officials from NIH told us they may apply specific award conditions such as additional reporting requirements to require correction of financial or administrative deficiencies identified during the pre-award risk review or at any point during the period of performance.

Some Agencies Take Additional Steps to Address Potential Risks in Providing R&D Funding to Foreign Entities of Concern

Almost all the agencies we interviewed—DOD, NASA, NIH, and NSF—reported that they have additional agency-specific requirements for

³⁰According to Treasury, under certain circumstances federal awarding agencies can apply for special licenses from the Office of Foreign Assets Controls (OFAC) to make awards that otherwise would be prohibited by certain sanctions.

³¹2 C.F.R. § 200.206(b)(1), 2 CFR 200.208, FAR 35.005, FAR 52.246-9.

Letter

awarding R&D funding when foreign entities of concern are involved. Most of these requirements either prohibit or restrict R&D funding to Chinese entities. For example, NASA is prohibited from providing funding for bilateral collaboration, participation, or coordination with China or Chinese-owned entities. DOD requires DOD contractors to disclose if any part of its workforce or facilities would be in China on certain acquisitions.

In addition, agencies have implemented their own requirements, guidance, and restrictions on awarding funds to entities in China and Russia in response to changes in the research security landscape (see table 5).

Table 5 provides information on agency-specific requirements when foreign entities of concern are or may be identified during the award vetting process.

Letter

Table 5: Key Agency-Specific Requirements for Awarding R&D Funding to Foreign Entities of Concern

Department of Defense (DOD)	Restriction on the acquisition of certain magnets, tantalum, and tungsten from North Korea, China, Russia, and Iran. Restricts contractors from purchasing any of these materials from these countries. (DFARS clause 252.225-7052). Restriction on the acquisition of personal protective equipment and certain other items from non-allied foreign nations. Prohibits contractors from providing specified items from North Korea, China, Russia, and Iran. This clause is generally required in solicitations and contracts for acquisition of these items, including for commercial items, that are for use in the U.S and have an estimated value of greater than \$150,000. (DFARS Clause 252.225-7061). Confucius Institutes. Beginning in FY 2024, unless a waiver is granted, no U.S. institution of higher education that hosts a Confucius Institute may receive DOD funding. Confucius Institutes are cultural institutes directly or indirectly funded by the government of the People's Republic of China. Disclosure of ownership or control by the government of a country that is a state sponsor of terrorism as determined by the Secretary of State under Section 1754(c)(1)(A)(i) of the Export Control Reform Act of 2018 (currently determined to include Iran and North Korea). According to DOD officials, this provision is required in solicitations, including for commercial products and commercial services that are expected to result in a contract valued at \$150,000 or more. Award is prohibited under this provision, unless a waiver is granted. (DFARS 252.225-7050). Disclosure of employment in the People's Republic of China is required for non-commercial contracts with a value of over \$5 million unless a waiver is granted. (DFARS Provision 252.225-7057, and DFARS Clause 252.225-7058).
Department of Energy (DOE)	DOE officials stated the agency does not provide any funding to foreign entities of concern identified during the award vetting process.
National Aeronautics and Space Administration (NASA)	Prohibition on funding (grants and contracts) that involves the bilateral participation, collaboration, or coordination with China or any Chinese entity. (Pub. L. No. 112-10, § 1340(a), Pub. L. No. 112-55, § 539, implemented through the NASA Grants and Cooperative Agreement Manual and NASA Procurement Class Deviation 12-01(A)).
National Institutes of Health (NIH)	Per NIH guidance, the agency obtains a U.S. State Department review of any potential award involving a "foreign component," including foreign entities of concern, in which any significant scientific work or segment of a project will be conducted outside of the United States, either by the recipient or by a researcher employed by a foreign organization, whether or not grant funds are expended. The review is obtained through NIH's Foreign Award and Component Tracking System (FACTS). In interviews, NIH officials noted that the State Department review includes various criteria, such as whether potential awards include entities in "politically sensitive areas" and whether the award could lead to "negative foreign policy implications" for the United States, among other things. If the State Department does not review an award within 14 days, a request is considered automatically approved except for awards to China or India; those awards must undergo State Department review.
National Science Foundation (NSF)	According to NSF officials, the agency obtains State Department review of all prime awards to foreign entities to ensure the funding does not raise foreign policy concerns. State Department officials we interviewed said they assess multiple risks during their review of NSF awards, including foreign entities on sanctions lists, such as the FTO and SDN lists, as well as identifying ties to entities in Russia and China.

Source: GAO analysis of agency information. | GAO-24-106227

Letter

In addition, some agencies we interviewed also told us they are taking or planning to take additional steps to mitigate their own research security risks from foreign entities, including those foreign entities of concern (see Table 6).³²

³²We asked the R&D federal awarding agencies in our review about any specific policies or guidance on monitoring subcontractors or subrecipients and subcontracts or subawards involving foreign entities of concern. The agencies stated that they have a relationship with a prime awardee and no direct relationship with a subcontractor or subrecipient. Awarding agencies stated that if a foreign subcontractor or subrecipient is identified in a proposal or application, the agency does also vet that potential subcontractor or subrecipient.

Letter

Table 6: Recent Agency-Specific Actions to Mitigate Risk in Awarding Research & Development Funding to Foreign Entities of Concern

Department of Defense (DOD)	In June 2023, DOD issued a new policy that requires DOD components to assess the risk of all fundamental research projects being considered for funding. The policy defines risk factors to be considered, such as whether the entity is actively receiving funding from a foreign country of concern. The policy also describes conditions under which funding is prohibited or where mitigation measures are required or recommended prior to issuing funding. Examples of mitigation measures include increasing the frequency of project reporting and removing individuals it deems research security risks. As part of this effort, DOD developed a risk matrix to guide program managers in assessing risks.
Department of Energy (DOE)	DOE officials said the agency is taking steps to evaluate research and development (R&D) awards for potential research security risks, including those posed by foreign entities of concern. For example, officials from one DOE program office explained that proposed R&D awards from their office are evaluated by DOE's Office of Counterespionage to identify whether personnel have connections to China, Russia, Iran, or North Korea. Officials from two other DOE program offices told us that they are considering new disclosure requirements to improve assessment of foreign ownership and control from countries of concern. According to DOE officials, in March 2023, DOE established the Office of Research, Technology, and Economic Security (RTES), which is responsible for enhancing DOE's existing vetting processes by working in coordination with program offices. Its purpose is to ensure that risks of undue foreign influence are considered early in the competitive process and throughout the life of a DOE supported project. This enhanced process integrates RTES reviews at three major points: 1) before the solicitation is released (to ensure the appropriate RTES provisions are included); 2) review of applications before selection; and 3) during the project implementation. The review considers potential risks associated with foreign ownership, control, or influence; improper influence of an individual, entity, or project; conflicts of interest/conflicts of commitment; intellectual property theft; supply chain, procurement, and physical threats.
National Aeronautics and Space Administration (NASA)	NASA officials said they review all awards with foreign entities, including those of concern, in light of broader U.S. national security and foreign policy priorities. NASA officials said they do not typically fund foreign entities to conduct research.
National Institutes of Health (NIH)	In September 2023, NIH updated its policy on foreign award reporting in response to a January 2023 report by the Health and Human Services Office of Inspector General. Under this update, NIH instituted a provision effective as of January 1, 2024, to require foreign subrecipients to provide copies of all lab notebooks, data, and documentation that supports the research outcomes described in the progress reports. NIH officials stated that the fiscal year 2024 Grants Policy Statement included in all NIH grant awards will include this updated requirement.
National Science Foundation (NSF)	NSF officials stated they are taking steps to evaluate all R&D awards for potential research security issues, including those posed by foreign entities of concern. For example, NSF said they have established an analytics capability to analyze information disclosed by the applicants to identify potential research security concerns, such as undisclosed funding from a foreign entity of concern. But NSF officials stated that the agency rarely provides direct funding to foreign entities.

Source: GAO analysis of agency documents and interviews. | GAO-24-106227

National Science Foundation (NSF) Efforts to Address Research Security Risks

NSF is leading several interagency efforts, along with DOD, DOE, and NASA, to address research security risks, including those posed by foreign entities of concern. For example, NSF recently announced the establishment of a Research Security and Integrity Information Sharing Analysis Organization (known as "SECURE") that will share best practices and information on security risks. The agency also announced in July 2023 a new program that will fund projects which assess strategies for identifying and mitigating research security risks. Such strategies could include the development of best practices and guidance.

Source: GAO analysis of agency information. | GAO-24-106227

Letter

To complement its new policy issued in June 2023, DOD recently developed a risk matrix as a guide to assist program managers and DOD components in reviewing fundamental research applications and proposals for potential conflicts of interest and conflicts of commitment. DOD officials noted that this matrix requires, recommends, or suggest that agency officials add risk mitigation measures, such as increased frequency of project reporting, when an individual on the award discloses receiving funds from China, Iran, North Korea, or Russia (see appendix III). Similarly, NSF officials told us they are also planning efforts to address research security risks posed by foreign entities of concern (see sidebar).

Selected Agencies Reported Facing Challenges with Determining Foreign Ownership

Officials from the R&D funding agencies we reviewed noted challenges in identifying if an entity might be "owned by, controlled by, or subject to the jurisdiction or direction of" China, Russia, Iran, or North Korea.³³ Two agencies told us they use a combination of intelligence information and commercial business analytics tools in attempts to identify foreign

³³Agencies generally consider "owned by, controlled by, or subject to the jurisdiction or direction of" as part of their overall review of entities' foreign ownership, control, or influence—referred to in this report as "foreign ownership." A U.S. company is considered under foreign ownership, control, or influence whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may affect adversely the performance of classified contracts. DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) January 1995, Department of Defense - Department of Energy - Nuclear Regulatory Commission - Central Intelligence Agency, U.S. Government Printing Office ISBN 0-16-045560-X.

Letter

Recent Commerce Definition of Foreign Ownership

In September 2023, the Department of Commerce issued a rule which includes a definition of entities "owned by, controlled by, or subject to the jurisdiction or direction of a covered nation (as defined in 10 U.S.C. 4872(d))"—i.e., Russia, China, North Korea, and Iran. Officials at Commerce told us this definition applies only to the program subject to the rule. The rule defines these entities as:

1. The person is: (A) a citizen, national, or resident of a covered nation and (B) located in a covered nation;
2. The person is organized under the laws of or has its principal place of business in a covered nation;
3. 25 percent or more of the person's outstanding voting interest, board seats, or equity interest is held directly or indirectly by the government of a covered nation; or
4. 25 percent or more of the person's outstanding voting interest, board seats, or equity interest is held directly or indirectly by any combination of the persons as described above.

Preventing the Improper Use of CHIPS Act Funding, 88 Fed. Reg. 65600-65619 (September 25, 2023) (to be codified in 15 C.F.R. pt. 231).

Source: Agency information. | GAO-24-106227

ownership during vetting of entities.³⁴ However, these efforts are agency-specific and not shared across the agencies we reviewed. In September 2023 the Commerce Department further defined "owned by, controlled by, or subject to the jurisdiction or direction" of a covered nation in its final rule applicable to its semiconductor incentives program contained in the CHIPS Act of 2022 (see sidebar).

Other agencies we reviewed stated that additional guidance could be beneficial for determining foreign ownership when vetting potential R&D funding awardees and for identifying risk mitigation options. For example, officials at DOE told us that guidance could (1) define the extent of ownership for when an entity is considered foreign owned (e.g., 25 percent or more) and (2) identify information potential R&D awardees should disclose on foreign ownership, control, or influence. Officials at NSF stated that they would benefit from guidance on the potential for foreign influence when a domestic awardee (e.g., a U.S. university) has a foreign-based campus (e.g., in China). OSTP officials told us that they are addressing such issues on a case-by-case basis at this time, but OSTP

³⁴Pursuant to the Corporate Transparency Act (CTA), starting in January 2024 certain entities incorporated or registered in the United States will be required to report to Treasury certain identifying information on their beneficial owners—the individuals who directly or indirectly own or control the company. However, strict confidentiality requirements on the information imposed by the CTA restricts certain federal agencies' access to the information. Only those agencies that are engaged in national security, intelligence, or law enforcement activities, federal functional regulators, or the Department of the Treasury—all subject to certain protocols—may access the information. Officials in Treasury's Financial Crimes Enforcement Network told us they are currently engaged in rulemaking regarding access to beneficial ownership information.

Letter

officials also stated that they are aware that federal awarding agencies face challenges in identifying and mitigating such risks.

The National Security Presidential Memorandum 33 (NSPM-33) issued in January 2021 details the role of OSTP, in coordination with the Director of National Intelligence and other agency heads as appropriate, to enhance the R&D enterprise's—including R&D agencies—awareness of research security risks and policies and measures for mitigating these risks. In January 2022, OSTP issued broad guidance implementing NSPM-33 addressing foreign risks to government supported research security.³⁵

This guidance does not address foreign ownership, control, or influence for potential R&D awardees. More recently, the Research and Development, Competition, and Innovation Act requires OSTP to, among other things, develop or revise a national strategy to improve U.S.

science, technology, research, and innovation competitiveness to support the national security strategy.³⁶ This strategy is to include a number of areas as practicable, including specific plans to safeguard research and technology funded, as appropriate, in whole or in part, by the federal government—including technologies critical to national security—from theft by foreign entities of concern. However, in September 2023 OSTP officials told us they plan to address issues related to foreign entities of concern broadly and do not anticipate addressing foreign ownership, control, and influence directly in the forthcoming strategy.

One key role of OSTP is to serve as a sounding board and conduit of information for agency officials seeking to understand, clarify, and shape science and technology-related policy objectives and priorities. Another is to help agencies coordinate and integrate their science and technology strategies and activities. As the lead for interagency coordination on science and technology policies, OSTP can help agencies collaborate

³⁵NSPM-33 directs actions to strengthen the protections of U.S. government supported R&D against foreign government interference and exploitation. *National Security Personnel Memorandum 33, Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, Jan. 2021.

³⁶Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, sub. C, §10612(b)-(c) 136 Stat. 1636-1640 (2022). National security strategy refers to the national security strategy required under section 108 of the National Security Act of 1947 (50 U.S.C. §3043). OSTP officials told us that they anticipate issuing this strategy after December 31, 2024.

Letter

and share information on identifying and addressing complex challenges with foreign ownership.

Leading practices for interagency collaboration note that a lead agency can provide direction and coordination on complex issues especially when the lead agency has ties to a center of influence, such as to the President or Congress.³⁷ Additionally, Standards for Internal Control state that management should identify, analyze, and respond to risks—including risk associated with changes in the external environment—related to achieving the defined objectives.³⁸ For example, evolving complex corporate structures for potential R&D awardees, including risks from often unknown foreign ownership, could put federally funded research and development results at risk for foreign influence or theft. Bringing together agencies to share information on such complex matters could better position agencies to more fully safeguard R&D funds. Further, such information sharing could help federal agencies effectively vet foreign entities of concern and identify potential risks more consistently and effectively across the federal government.

Conclusions

OSTP has an important role to play in enhancing agencies' awareness of and collaboration on complex risks and challenges with research security such as identifying and addressing foreign ownership when making decisions about funding R&D. While OSTP has issued broad guidance on addressing foreign risks to federal research security, the guidance does not address foreign ownership. Additionally, an upcoming strategic document also will not specifically address this issue. We found two agencies that have used analytical tools in attempts to identify foreign ownership during vetting of entities; however, these efforts are agency-specific and not consistent across the agencies we reviewed. By bringing together federal awarding agencies to share information on identifying foreign ownership, OSTP could help facilitate a more consistent and effective approach to safeguarding U.S. R&D from foreign entities of concern.

³⁷GAO, *Government Performance Management: Leading Practices to Enhance Interagency Collaboration and Address Crosscutting Challenges*, [GAO-23-105520](#) (Washington, D.C.: May 24, 2023).

³⁸GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

Letter

Recommendation for Executive Action

As part of OSTP's ongoing efforts to address research security risks, the Director of OSTP, in coordination with federal R&D awarding agencies, should facilitate the sharing of information on identifying foreign ownership, control, or influence. This could occur, for example, in conjunction with OSTP's existing efforts to support the national security strategy or its existing role to enhance the federal research agencies' awareness of research security risks and policies under NSPM-33. (Recommendation 1)

Agency Comments

We provided a draft of this report to Commerce, DOD, DOE, DOJ, HHS, NASA, NSF, OSTP, GSA, State, and Treasury for review and comment. In an email response on December 21, 2023, OSTP officials stated they concur with our recommendation. Commerce, DOD, DOJ, HHS, NASA, NSF, and Treasury provided technical comments that we incorporated as appropriate. Officials from State, GSA, and DOE stated via email that they had no comments on the report.

We are sending copies of this report to the appropriate congressional committees; the Secretaries of Commerce, Defense, Energy, Health and Human Services, State, and Treasury; the Administrators of NASA and the GSA; the Attorney General; the Director of the NSF; the Director of the White House Office of Science and Technology Policy; and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6888 or WrightC@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



Candice N. Wright

Letter

Director, Science, Technology Assessment, and Analytics

Letter

List of Committees

The Honorable Maria Cantwell
Chair
The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate
The Honorable Benjamin Cardin
Chairman
The Honorable James E. Risch
Ranking Member
Committee on Foreign Relations
United States Senate
The Honorable Bernard Sanders
Chairman
The Honorable Bill Cassidy
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate
The Honorable Cathy McMorris Rodgers
Chair
The Honorable Frank Pallone, Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives
The Honorable Michael McCaul
Chairman
The Honorable Gregory Meeks
Ranking Member
Committee on Foreign Affairs
House of Representatives
The Honorable Frank Lucas
Chairman
The Honorable Zoe Lofgren
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The Research and Development, Competition, and Innovation Act (the Act) passed in August 2022 includes provisions for GAO to report on research funding to foreign entities of concern and requirements for awarding, tracking, and monitoring of such funding.¹ This report: (1) describes challenges faced in identifying research and development (R&D) funds made available to foreign entities of concern and how much funding was made to foreign entities of concern in fiscal year (FY) 2017 through FY 2022 and (2) examines the requirements for awarding and monitoring² of such funding. We used FY 2017 through FY 2022 to cover the review time frame required by the Act.

For the first objective, we interviewed agency officials at the Office of Science and Technology Policy on the guidance they have issued and are developing for federal agencies on research security issues. We also interviewed officials at the Departments of State, Commerce, Justice, and the Treasury to gather information on their processes for identifying, classifying, and providing public information on foreign entities of concern as defined by the Act, including availability or reliability of identifying information such as address, date of birth, or passport number. We also interviewed officials at the General Services Administration (GSA) to identify their process for including information about foreign entities of concern in the System for Award Management (SAM.gov) and how SAM.gov registrant information links to USAspending.gov. We queried officials at each of these agencies on their knowledge of federal awarding agencies' access to quality information about foreign entities of concern. We then obtained and analyzed information on the foreign entities and on federal R&D award funding data, as follows:

1. *Amount of funding to foreign entities—individuals or organizations—listed on the Foreign Terrorist Organization (FTO) list and the Specially Designated Nationals and Blocked Persons (SDN) list.*

¹Research and Development, Competition, and Innovation Act, Pub. L. No. 117-167, div. B, tit. VI, sub. D, §10635, 136 Stat. 1366, 1668-69 (2022).

²For the purposes of this report, "monitoring" includes both monitoring and tracking of funds.

-
- **Foreign Terrorist Organization list:** We collected publicly available information on entities designated as a foreign terrorist organization by the Secretary of State under section 219(a) of the Immigration and Nationality Act (8 U.S.C. §1189(a)) and maintained by the Department of the State on the agency website.³ The website lists 75 organizations designated as FTOs from FY 2017 through FY 2022.
 - **Specially Designated Nationals.** We reviewed publicly available information on the list of specially designated nationals and blocked persons maintained by the Office of Foreign Assets Control (OFAC) of the Department of the Treasury (commonly known as the SDN list) from the agency website. In August 2023 we downloaded a machine-readable version of the SDN from OFAC's website.⁴ We then engaged in a parsing and cleaning process intended to return a list of searchable entity names, which would maximize the probability of identifying those entities in an arbitrary third-party data system.

For individuals on the SDN list, we used both surname-given name and given name-surname order to build separate search strings. We also built search strings using OFAC-provided "also known as" (AKA) identities. For other types of entities on the SDN list, we removed excess punctuation and various corporate substrings (e.g., "Corp" or "Inc"). For all SDN list entities, we omitted OFAC-identified "vessels" and search strings with character lengths of less than 7. We also omitted a small number of selected entities that produced very large numbers of clearly irrelevant results when searched in USAspending.gov.
 - **Foreign Entities Convicted under Specified Federal Laws.** We also collected information on entities—individuals and organizations—convicted under the laws identified in the Act from the Department of Justice (DOJ) from FY 2017 through FY 2022.⁵ DOJ officials stated that the total number of convictions under these statutes (518) included some "sealed" cases for which providing case-specific information would violate a court order. Therefore, the total number of cases for which DOJ provided information to GAO was 483 (excluding

³<https://www.state.gov/foreign-terrorist-organizations/>.

⁴<https://ofac.treasury.gov/specially-designated-nationals-list-data-formats-data-schemas>.

⁵We met with DOJ officials to ascertain the extent to which the department has identified and maintains an available data set of entities "alleged by the Attorney General to have been involved in activities for which a conviction was obtained" under the laws specified in the Act. DOJ officials told us that while DOJ may have information on such entities, it is not compiled in a usable and shareable format. Therefore, we looked at entities convicted under these specified laws.

sealed cases). We then excluded entities identified in DOJ data as U.S. citizens and used the data on the remaining entities in our data analysis as described below.

We searched USAspending.gov to identify whether R&D funds were provided to these entities. Specifically, we searched for matches—in the names of entities on the lists (such as the SDN list) and addresses—with similar information for award recipients in USAspending.gov to determine whether any foreign entities of concern received R&D funds during the 6-year period.

- For the SDN entities, we ran the resulting (approximately 41,000) text strings through the USAspending.gov application programming interface (API) to obtain unique recipient identifiers. We then used those identifiers to find matching SDN list entities, resulting in 8,125 recorded matches. We also used the returned data to programmatically assign confidence levels to matches.

We applied the same programmatic cleaning to the USAspending.gov name strings as we had previously applied to the SDN search strings. We identified 'high' confidence levels based on whether there were exact matches across the edited SDN list search strings and the edited USAspending.gov recipient name strings. We applied 'medium' confidence levels based on whether, accounting for spaces and other delimiters, the SDN list search strings appeared as exact substrings of the USAspending.gov name strings.⁶

Based on this analysis, we identified 1,084 relatively high-confidence name matches. We conducted manual review and analysis to determine if the addresses of the USAspending.gov recipients matched available address information for the SDN entities and found one likely match. We queried USAspending.gov on that entity and found no agency-reported funding within our allotted time frame from FY 2017 through FY 2022.

- We conducted a similar process for the 483 convicted entities provided by DOJ. We eliminated those with a citizenship listed as "United States" to focus on foreign entities. To the extent we were able to locate addresses for these entities through the Public Access to Court Electronic Records website, we used that information to

⁶For example, if an SDN list search string was "ABC Corp" and the USAspending.gov name string was "ABC Corp Inc", it would be assigned a medium confidence. However, if the USAspending.gov name string was "ABC Corporation Inc", it would be assigned a low confidence because the 2nd space-delimited word did not match exactly to that of the SDN list equivalent.

Appendix I: Objectives, Scope, and Methodology

determine if it matched the address information for the award recipient in USAspending.gov with the possible name match. We found no matches.

2. *Amount of funding reported by U.S. agencies through prime awards to entities located in China, Iran, North Korea, and Russia.*

Due to the difficulty of determining whether an entity is "owned by, controlled by, or under the jurisdiction of" China, Iran, North Korea and Russia, we assessed USAspending.gov data for award recipients located in these countries. We examined the amount, type, and purpose of funds obligated⁷ by U.S. agencies to entities located in China (including Hong Kong), Iran, North Korea and Russia referred to as covered nations⁸ by analyzing prime award data⁹ from USAspending.gov.¹⁰ Our scope covered prime awards (grants, cooperative agreements, and contracts) made directly to an entity in a covered nation from FY 2017 through FY 2022.¹¹ GAO has reported on challenges and limitations with the quality of USAspending.gov

⁷An obligation is a definite commitment that creates a legal liability of the government for the payment of goods and services ordered or received, or a legal duty on the part of the United States that could mature into a legal liability by virtue of actions on the part of the other party, beyond the control of the United States. Payment may be made immediately or in the future. For amounts identified, in USAspending.gov we used the "federal action obligation" field to calculate amounts obligated to these awards between FY 2017 and FY 2022.

⁸10 U.S.C. § 4872 defines "covered nations" as the Democratic People's Republic of North Korea, the People's Republic of China, the Russian Federation, and the Islamic Republic of Iran.

⁹For the purposes of this report, we define a prime award as contract, grant, or cooperative agreement that the U.S. government awards directly to a non-federal entity for the purpose of carrying out a federal program.

¹⁰Agencies are required to report certain information about federal awards that equal or exceed the micro-purchase threshold which is then made available to the public on a single public-facing, searchable website. The USAspending.gov website is the official public source of spending data submitted by U.S. agencies. Federal Funding Accountability and Transparency Act of 2006, Pub. L. No. 109-282, 120 Stat. 1186 as amended by The Digital Accountability and Transparency Act of 2014, Pub. L. No. 113-101, 128 Stat. 1146 (codified as amended at 31 U.S.C. § 6101 note); 2 C.F.R. pt. 170, FAR subparts 4.6 and 4.14. Department of the Treasury, <https://www.usaspending.gov>, accessed September 8 and 23, 2023.

¹¹We analyzed USAspending.gov data as of September 8, 2023, for China and Russia and as of September 23, 2023, for Iran and North Korea. We included 6 fiscal years from 2017 through 2022 in the scope of this review.

Appendix I: Objectives, Scope, and Methodology

subaward data, and we did not analyze subaward data for entities located in the four countries.¹²

We analyzed the prime award data in USAspending.gov by agency, federal action obligation amount, fiscal year, award recipient, recipient location, sector code and description, and prime base award description.¹³ In some instances there were data missing in the "award type" field; we reviewed corresponding data in the "award type code" data field for the award to populate missing data in the "award type" field. We conducted logical tests on the data for missing data or outliers. We provided our analysis to the relevant agencies to verify its accuracy, the agencies provided corrections where necessary, and we incorporated these corrections into our final analysis. We interviewed agency officials as necessary to understand these corrections, which officials attributed to accuracy of either "non-R&D activities" that were not reflected in the USAspending.gov data or miscoding a cooperative agreement as a grant. We determined that the USAspending.gov data, after incorporating the agency corrections, were sufficiently reliable for the purposes of summarizing obligation amounts through prime awards.

For the second objective, we focused on the five agencies that—according to an April 2022 report by the National Science Foundation (NSF)—obligated the largest amount of R&D funding in FY 2020.¹⁴ FY 2020 data were the most recent available when we initiated this review. The five agencies are: the NSF; the Departments of Defense (DOD), Energy (DOE), and primarily the National Institutes of Health (NIH) within Health and Human Services (HHS); and the National Aeronautics and Space Administration (NASA). We collected agency policies and other documents and interviewed agency officials on requirements for awarding and monitoring federal funds to foreign entities of concern. To determine whether a specific requirement was related to a foreign entity of concern, we analyzed each requirement reported by each funding agency to

¹²GAO, *Federal Spending Transparency: Opportunities to Improve USAspending.gov Data*, GAO-24-106214 (Washington, D.C.: Nov. 7, 2023).

¹³To identify the sector code, we used the North American Industry Classification System (NAICS) manual for 2022—the standard system for classifying contract codes—and the Annual Publication of Assistance Listings for 2022 (previously called the Catalog of Federal Domestic Assistance and still commonly referred to as CFDA codes). Specifically, we searched for terms including "research," "development," and "science," to identify an award as an R&D award.

¹⁴National Science Foundation, National Center for Science and Engineering Statistics, *Federal Funds for Research and Development* (Alexandria, Va.: Apr. 28, 2022).

identify whether the requirement specifically referenced one or more of the entities in our mandate, such as a foreign terrorist organization, or one of the four covered nations (e.g., China), or if foreign entities of concern were specifically covered by the requirement.

We also conducted a key word search of laws, federal acquisition regulations, and government-wide guidance for grants and agreements for additional government-wide requirements for awarding and monitoring specific to foreign entities of concern. To do this, we conducted key word searches in searches in the Federal Acquisition Regulation and subtitle A of chapter 2 of the Code of Federal Regulations, and we searched a legal database based on the definition of foreign entity of concern, such as searching for terms like "foreign terrorist organization."

We analyzed identified requirements to determine whether each requirement applied to all federal R&D funding agencies or to a specific R&D funding agency. We also analyzed policy documents from the five R&D funding agencies in our scope to determine what, if any, processes each agency has in place for reviewing R&D awards with foreign entities. We interviewed agency officials to obtain greater insight into their processes and policies, including forthcoming changes to them. We also asked about additional steps, if any, they take to vet entities for awards involving foreign entities of concern.

We conducted this performance audit from August 2022 to January 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for any findings and conclusions based on our audit objectives.

Appendix II: Research and Development (R&D)
Federal Funding Obligated to Entities Located
in China and Russia

Appendix II: Research and Development (R&D) Federal Funding Obligated to Entities Located in China and Russia

As shown in Table 7, multiple U.S. federal agencies obligated funds for R&D awards made directly from a federal agency to entities located in China and Russia from fiscal years 2017 through 2022. These awards included grants, cooperative agreements, and contracts.

Table 7: Obligations Funded in Fiscal Years 2017-2022 for Research & Development Awards Made Directly to Entities Located in China^a and Russia

Amount in thousands of dollars

Recipient location Country	Awarding agency	Recipient	Award type	Award description	Obligations in fiscal years 2017-2022
China	Centers for Disease Control and Prevention	Chinese Center for Disease Control and Prevention	Cooperative agreement	Conducting public health research in China	1,197
China	Centers for Disease Control and Prevention	Chinese Center for Disease Control and Prevention	Cooperative agreement	Public health epidemiology of influenza virus infection and control in China	3,539
China	Centers for Disease Control and Prevention	University of Hong Kong	Cooperative agreement	Research on the epidemiology, vaccine effectiveness, and treatment of influenza and other respiratory viruses in Southeast Asia and the western Pacific	9,400
China	Department of Agriculture	Wuhan Botanical Garden, Chinese Academy of Sciences	Cooperative agreement	Biological control of Japanese stiltgrass	34
China	Department of Agriculture	Nanjing Agricultural University	Cooperative agreement	Evaluation of the potential and host-specificity testing of pathogens as bio-control agents against <i>Microstegium vimineum</i>	55
China	Department of Agriculture	Fujian Agriculture and Forestry University	Cooperative agreement	To develop survey techniques determining the distribution and risk factors of <i>Lymantria</i> spp.	33

**Appendix II: Research and Development (R&D)
Federal Funding Obligated to Entities Located
in China and Russia**

Recipient location Country	Awarding agency	Recipient	Award type	Award description	Obligations in fiscal years 2017-2022
China	Department of Agriculture	Chinese Academy of Forestry	Cooperative agreement	To collaborate on research to discover and collect parasitoids of the Asian longhorned beetle and the spotted lanternfly	91
China	Department of Agriculture	Fujian Agriculture and Forestry University	Cooperative agreement	To develop survey techniques determining the distribution and risk factors of <i>Lymantria</i> spp.	39
China	Department of Agriculture	Chinese Academy of Forestry	Cooperative agreement	Host range and reference and evaluation of insecticide treatment	66
China	Department of Agriculture	Chinese Academy of Forestry	Cooperative agreement	Exploration for Asian longhorned beetle and the spotted lanternfly parasitoids in China	210
China	Department of Agriculture	Fujian Agriculture and Forestry University	Cooperative agreement	Characterize risks of exotic <i>Lymantria</i> species in south China	46
China	Department of Agriculture	Beijing Forestry University	Cooperative agreement	Risk characterization of <i>Lymantria</i> and light trap evaluation of Asian gypsy moth	39
China	Department of Agriculture	Chinese Academy of Forestry	Cooperative agreement	Host range and preference of the Asian longhorned beetle	61
China	Department of Agriculture	Fujian Agriculture and Forestry University	Cooperative agreement	Risk characterization and mitigation of <i>Lymantria</i> in southern China	73
China	Department of Agriculture	Chinese Academy of Forestry	Cooperative agreement	Research to discover natural enemies that could be used to assist in the control of the exotic invasive spotted lanternfly.	37
China	Department of Agriculture	Chinese Academy of Agriculture Plant Protection Research Institute	Cooperative agreement	Exploration for natural enemies of invasive species originating from China and the surrounding areas that affect Chinese and U.S. agriculture	357
China	Department of Agriculture	Chinese Academy of Agriculture Plant Protection Research Institute	Cooperative agreement	Distribution and natural enemy complex of Roseau cane scale in China	24
China	Department of Agriculture	Wickham, Jacob	Cooperative agreement	Develop new and improved attractants and trapping methods for wood-boring beetles from China, with emphasis on longhorned beetles	90
China	Department of Agriculture	Ecology and Nature Conservation Institute, Chinese Academy of Forestry	Grant	Biological control of invasive Asian longhorned beetle	21
China	Department of Agriculture	China Academy of Agriculture Plant Protection Research Institute	Grant	Distribution and natural enemy complex of Roseau cane scale in Asia	24

**Appendix II: Research and Development (R&D)
Federal Funding Obligated to Entities Located
in China and Russia**

Recipient location Country	Awarding agency	Recipient	Award type	Award description	Obligations in fiscal years 2017-2022
China	Department of Agriculture	Nanjing Agricultural University	Grant	Microstegium vimineum rust fungi as biological control agents	20
China	Department of Defense	University of Hong Kong	Grant	Compressive feedback for featureless video-based tracking control	100
China	Department of Defense, Army	University of Hong Kong	Grant	Compressive feedback for featureless video-based tracking control	75
China	Department of the Interior	Wildlife Conservation Society	Grant	Develop a new portable DNA-based genetic test tool that will enhance enforcement of international regulations and lead to a reduction in big cat trafficking	70
China	HHS Office of the Assistant Secretary for Health	University of Hong Kong	Grant	6th world conference on research integrity	50
China	National Institutes of Health	Cancer Hospital, Chinese Academy of Medical Sciences	Contract	Nutrition intervention trial biobank	75
China	National Institutes of Health	Cancer Hospital, Chinese Academy of Medical Sciences	Contract	Upper gastrointestinal cancer prevention studies	365
China	National Institutes of Health	Beijing George Medical Research Co. Ltd.	Cooperative agreement	Integrating depression care for ACS patients in low-resource hospitals in China	300
China	National Institutes of Health	National Center for Aids/Std Control and Prevention, Chinese Center for Disease Control and Prevention	Cooperative agreement	HIV/AIDS clinical trial unit in NCAIDS	0 ^b
China	National Institutes of Health	National Center for Aids/Std Control and Prevention, Chinese Center for Disease Control and Prevention	Grant	Strengthening research integrity oversight and ethical review of critical HIV research in China	298
China	National Institutes of Health	Peking University	Grant	China health and retirement longitudinal study	5,298
China	National Institutes of Health	Peking University	Grant	Harmonized cognitive and dementia assessment in China	1,323
China	National Institutes of Health	Institut Pasteur of Shanghai, Chinese Academy of Sciences Wuhan University	Grant	Versatile functions of LANA in KSHV pathogenesis	303

**Appendix II: Research and Development (R&D)
Federal Funding Obligated to Entities Located
in China and Russia**

Recipient location Country	Awarding agency	Recipient	Award type	Award description	Obligations in fiscal years 2017-2022
China	National Institutes of Health	Institut Pasteur of Shanghai, Chinese Academy of Sciences	Grant	Var gene regulation mechanisms in malaria parasite <i>Plasmodium falciparum</i>	389
China	National Institutes of Health	Fudan University	Grant	Influence of gut microbiota on vector competence of disease transmitting insects	730
China	National Institutes of Health	Southern Medical University	Grant	Impacts of urbanization on vector biology and transmission of dengue in China	667
China	National Institutes of Health	China Medical University	Grant	Antigen discovery for transmission-blocking vaccines in <i>plasmodium vivax</i>	407
Russia	Department of Agriculture	VNIIR, FGBU	Cooperative agreement	Asian gypsy moth	188
Russia	Department of Agriculture	VNIIR, FGBU	Cooperative agreement	Asian gypsy moth	188
Russia	Department of Agriculture	VNIIR, FGBU	Cooperative agreement	Asian gypsy moth at Russian ports	188
Russia	Department of Commerce	Yakut Administration for Hydrometeorology and Environmental Monitoring	Contract	Upper air data collection at the Tiksi observatory in Russia	275
Russia	Department of Commerce	Arctic and Antarctic Research Institute, Federal State Budgetary Institution	Contract	Transmission of atmospheric data from the Tiksi observatory in Russia	68
Russia	Department of Defense	International Science and Technology Center	Contract	Summary - kickoff meeting	302
Russia	Department of the Interior	Sovet Po Morskim Mlekopitayushchim Oo	Cooperative agreement	Amendment to provide additional travel funds	12
Russia	Department of the Interior	Zoological Society of London	Grant	Rhino Tiger-FY 17-RT1727 ^c	104
Russia	Department of the Interior	Fond Phoenix	Grant	Rhino Tiger-FY 17-RT1701 ^c	24
Russia	Department of the Interior	Zoological Society of London	Grant	RT1832 ^c	100
Russia	Department of the Interior	Fond Phoenix	Grant	Encouraging locals to support Amur tiger recovery in northern range	25
Russia	Department of the Interior	Wildlife Conservation Society	Grant	Smart anti-poaching in protected and unprotected tiger habitat in Russia	60

Source: GAO analysis of data in USAspending.gov, accessed and downloaded September 8, 2023. | GAO-24-106227

Note: Dollar amounts are rounded. Also, some of the award recipients we identified are under the jurisdiction or direction of the governments of China and Russia. For example, direct funds were provided to the Chinese Center for Disease Control and Prevention and the Russian Ministry of Natural Resources and Environment (Yakut Administration for Hydrometeorology and Environmental

**Appendix II: Research and Development (R&D)
Federal Funding Obligated to Entities Located
in China and Russia**

Monitoring). We did not verify ownership or control for all the recipients we identified due to challenges with determining foreign ownership as we discussed in this report.

^aWe included federal research funds provided to entities in Hong Kong, a Special Administrative Region of China, due to the recent change in the treatment of the region by the U.S. government. In July 2020, the President determined in Executive Order 13936 that Hong Kong was no longer sufficiently autonomous to justify differential treatment in relation to China. Specifically, the President suspended the application of section 201(a) of the United States-Hong Kong Policy Act of 1992 to several specified statutes.

^bAccording to NIH officials, \$1 was funded to this recurring award to keep it active in the Department's and agency's internal systems. No other funding was obligated under this award within the scope of our review.

^cUSAspending.gov did not provide information on the description of this award. According to the Department of the Interior's public website, the Rhinoceros and Tiger Conservation Fund provides financial and technical support to projects that deliver measurable conservation results for African and Asian rhinoceros and tiger populations in Asia.

Appendix III: Examples of Information Used by
the Department of Defense to Inform
Fundamental Research Mitigation Decisions

Appendix III: Examples of Information Used by the Department of Defense to Inform Fundamental Research Mitigation Decisions

Table 8 provides examples of information used by DOD to inform
fundamental research mitigation decisions.

Table 8: Examples of Information Used by the Department of Defense (DOD) to Assess a Covered Individual's Associations, Affiliations, and Collaborations and the Policies of the Proposing Institution that Employs the Covered Individual

	Foreign Talent Recruitment Programs	Funding Sources	Patents	Entity Lists
Mitigation Required ^a	Indicators of participation in a foreign talent recruitment program (FTRP) for the period after August 9, 2024. ^b	Indicators of current funding from a country of concern. ^c	Patent applications or patents not disclosed in proposal that result from research funded by the U.S. government (USG) that were filed in a foreign country of concern (FCOC) prior to filing in the United States or filed on behalf of an FCOC connected entity.	Indicators of affiliation with an entity on the denied entity or person list – trade restriction lists published by Commerce's Bureau of Industry and Security (BIS) consisting of some foreign entities of concern.
Mitigation Measures Recommended	Policy of proposing institution employing applicant does not prohibit participation in a malign foreign talent recruitment program (MFTRP). ^d	Indicators of past funding from a country of concern.	Patent applications or patents disclosed in proposal resulting from research funded by the USG that were filed in an FCOC prior to filing in the United States or on behalf of an FCOC connected entity.	N/A ^e
Mitigation Measures Suggested	Applicant's co-author on publications in scientific and engineering (S&E) journals are participants in a MFTRP or FTRP.	Indicators of limited or partial funding from a country of concern.	Patent applications or patents not disclosed in fundamental research project proposal that result from research funded by USG that were filed in a non-FCOC prior to filing in the United States or on behalf of an entity in a non-FCOC. Co-patent applicant with a person on the U.S. BIS Denied Persons List.	Applicant is co-author on a publication in a S&E journal affiliated with an entity on the BIS lists.
No Mitigation Needed	No indicators of participation in a MFTRP or FTRP.	No indicators of current or past funding from a country of concern.	All patent applications or patents resulting from research funded by the USG have been filed in the United States prior to filing in any other country.	No Indicators of any association or affiliation with an entity on the BIS lists.

**Appendix III: Examples of Information Used by
the Department of Defense to Inform
Fundamental Research Mitigation Decisions**

Source: GAO analysis of risk matrix from DOD. | GAO-24-106227

^aDOD's June 2023 decision matrix states that the proposal must be rejected if no mitigation is possible.

^bThe National Science and Technology Council implementation guidance for National Security Presidential Memorandum 33 defines a foreign government-sponsored talent recruitment program as an effort organized, managed, or funded by a foreign government, or a foreign government instrumentality or entity, to recruit science and technology professionals or students.

^cDOD defines a country of concern as China, Russia, North Korea, and Iran.

^dDOD's June 2023 decision matrix states that beginning in August 2024 any indicators of participation in a foreign talent recruitment program, as defined in the Chips and Science Act, will automatically disqualify an applicant from receiving funding.

^ePrior to August 2022 mitigation measures were recommended when indicators of affiliation with an entity on the BIS lists were present. Since August 2022 mitigation measures are required in these instances.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Candice Wright at (202) 512-6888 or wrightc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Farahnaaz Khakoo-Mausel (Assistant Director), Sharron Candon (Analyst-in-Charge), Ebony Russ, and Courtney Thacker made key contributions to this report. In addition, Jenny Chanley, Louise Fickel, Ryan Han, Gabriel Nelson, Flora Ngo, and Amy Pereira contributed to the report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).

Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).

Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.

